

Segurança da informação

Ficha Técnica

MINISTÉRIO DE TRABALHO

Ministro do Trabalho

Ronaldo Nogueira

Secretário de Políticas Públicas de Emprego

Leonardo José Arantes

Diretor do Departamento de Políticas de Empregabilidade

Higino Brito Vieira

Chefe da Assessoria de Comunicação Social (ASCOM)

Angelo Marcio Fernandes de Sousa Filho

UNIVERSIDADE DE BRASÍLIA

Reitora

Márcia Abrahão Moura

Vice-reitor

Enrique Huelva

Decana de Pesquisa e Inovação

Maria Emilia Machado Telles Walter

Decana de Extensão

Olgamir Amancia

Coordenação do Projeto Qualifica Brasil

Thérèse Hofmann Gatti Rodrigues da Costa (Coordenadora Geral)

Wilsa Maria Ramos

Valdir Adilson Steinke

Luis Fernando Ramos Molinaro

Humberto Abdalla Júnior

Rafael Timóteo de Sousa Jr

Instituto Brasileiro de Informação em Ciência e Tecnologia – IBICT

Cecília Leite - Diretora

Tiago Emmanuel Nunes Braga

Realização

Instituto de Artes (IDA-UnB), Instituto de Psicologia (IP-UnB), Instituto de Letras (LET-UnB), Departamento de Engenharia Elétrica (ENE – UnB), Departamento de Geografia (GEA – UnB), Faculdade de Ciência da Informação (FCI-UnB).

Apoio

Secretaria de Educação Profissional e Tecnológica (SETEC-MEC)

Gestão de Negócios e Tecnologia da Informação

Lourene Rapôso Oliveira Garcez

Wellington Lima de Jesus Filho

Coordenação da Unidade de Pedagogia

Danielle Nogueira Pamplona

Livia Veleda Sousa e Melo

Gerente do Núcleo de Produção de Materiais

Rute Nogueira de Moraes Bicalho

Autor

Igor dos Santos Rodrigues

Equipe de Designer Instrucional

Rute Nogueira de Moraes Bicalho

Janaína Angelina Teixeira

Márlon Cavalcanti Lima

Simone Escalante Bordallo

Virgínia Maria Soares de Almeida

Marcus Vinicius Carneiro Magalhães

Revisor ortográfico

Samantha Resende Nascimento

Ilustrador

Ana Maria Silva Sena Pereira

Desenvolvedor de Vídeos Animados

Paulo Fernando Santos Nisio

Desenvolvedor de Ambiente Virtual de Aprendizagem

Osvaldo Corrêa

Projeto Gráfico

Márlon Cavalcanti Lima



Este material foi produzido por conteudista(s) da Universidade de Brasília (UnB) exclusivamente para a Escola do Trabalhador. Licença de uso e compartilhamento Creative Commons Atribuição-Não Comercial – Sem Derivações 4.0 Internacional. <http://creativecommons.org/licenses/by-nc-nd/4.0/>

O que você vai estudar

Tema 1

Introdução ao assunto
Segurança da Informação

Tema 2

Princípios e conceitos da
Segurança da Informação

Tema 3

Gestão de processos de
segurança

Apresentação

Somos diariamente expostos aos meios tecnológicos como: celular, computador, *tablets* e câmeras digitais. Consequentemente, estamos constantemente passando informações para esses meios tecnológicos, como: informações pessoais, dados bancários e fotos. Essas informações são tão importantes para nós, como para as empresas, que recebem essas informações e ficam responsáveis pela guarda e preservação.

Deste modo, o estudo da segurança da informação é importante atualmente, sendo fundamental aprendermos mais sobre o assunto para proteger a organização de futuras ameaças.

Nosso objetivo é apresentar a importância da segurança da informação, atualmente, mostrar o quão necessário são as medidas de segurança para a competitividade de uma organização e também para sua vida pessoal. Neste sentido, esse curso será constituído de três unidades temáticas que abordarão desde uma introdução geral à Segurança da Informação até o como fazer a gestão de processos de segurança.

Tema 1

Introdução ao assunto



Bem-vindos ao curso de Segurança da Informação! Serei seu principal guia nessa jornada. Pronto para iniciarmos?

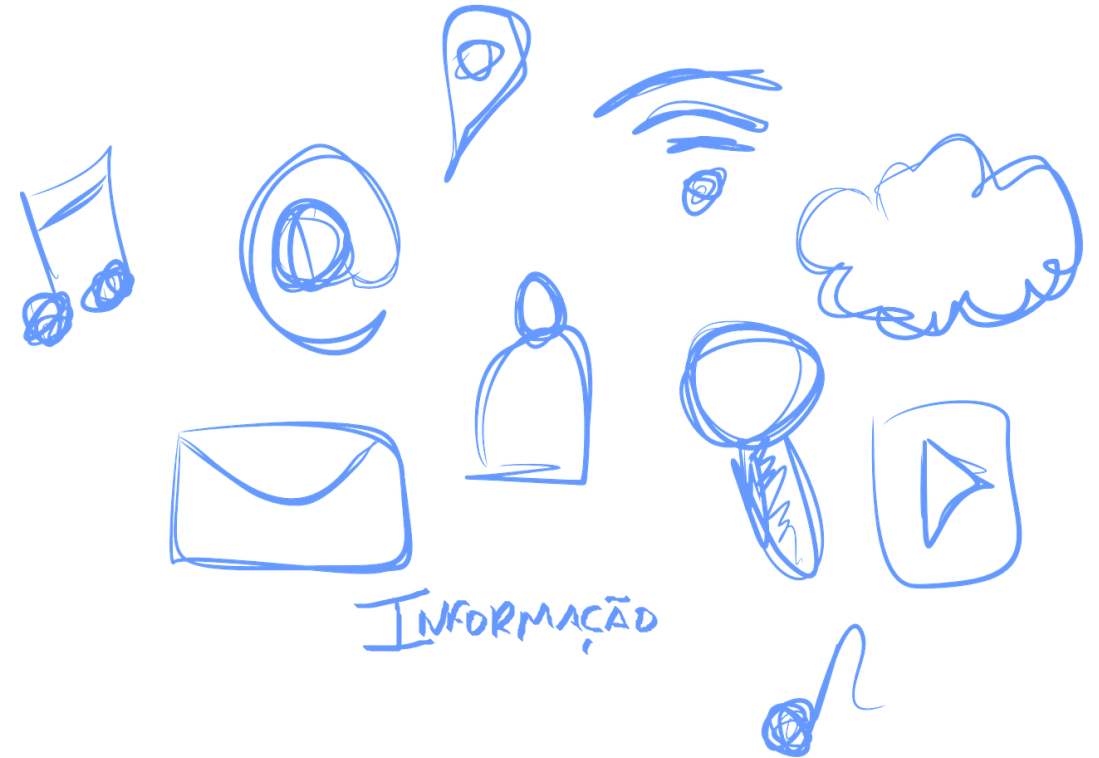
Para entendermos sobre o conceito de segurança da informação devemos compreender os termos separadamente. Logo, será retratado uma introdução assunto segurança da informação, por meio do estudo dos conceitos de **informação** e seu contexto histórico; **tecnologia da informação** e sua importância para as organizações e **segurança da informação** e a necessidade nos dias atuais.

O que é informação?

A Informação tem diversas definições. Conceitualmente, a **informação é um conjunto organizado de dados capazes de reduzir as incertezas ou incrementar o conhecimento** sobre algo, ou seja, a informação pode ser: um comunicado, que foi repassado pelo seu colega de trabalho; um aviso deixado na sua mesa; as notícias apresentadas em jornais e até mesmo o conteúdo dessa aula é uma informação. Como vimos, a informação como conceito **traz muitos significados** do uso mais cotidiano até o uso mais técnico.

Vamos entender um pouco melhor o que é informação por meio do entendimento de três aspectos:

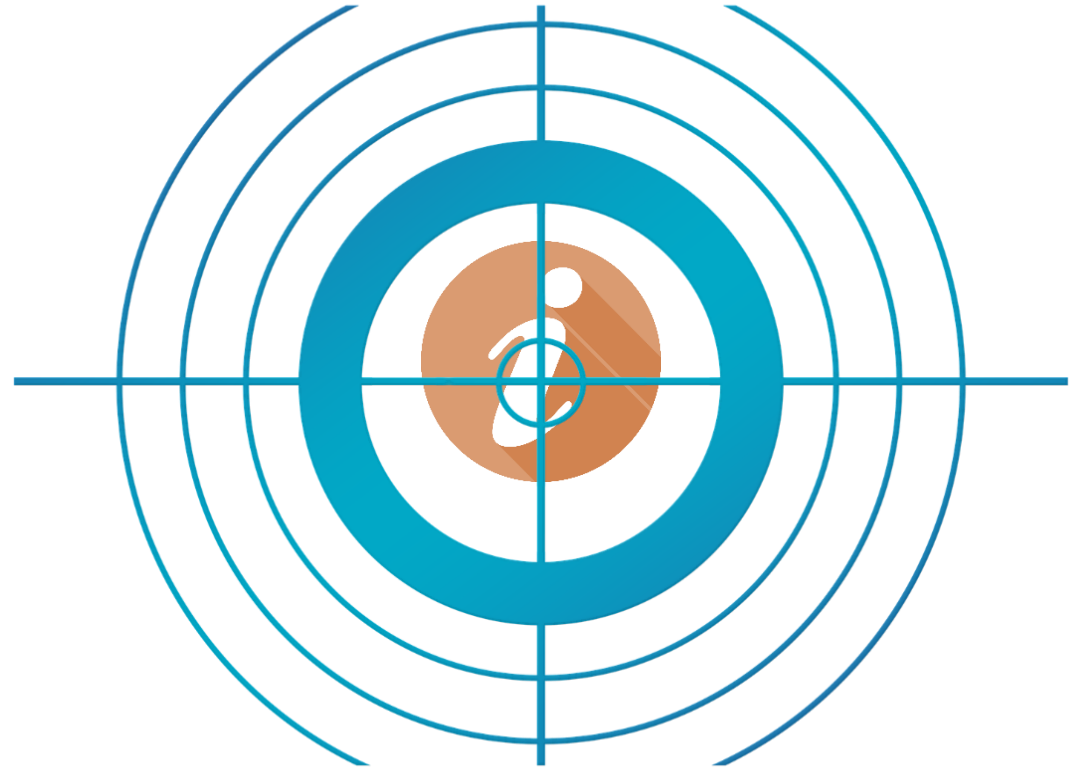
- » Relevância.
- » Comunicação.
- » Transferência do conhecimento.



O que é informação?

Relevância da Informação

A relevância da informação também **aplica um valor a ela**, por exemplo se eu te perguntar sobre um segredo você não vai querer me contar pois ele tem uma importância para você, agora se eu perguntar seu nome você provavelmente não recusará me dizer. Ambos os exemplos, tanto o segredo como o seu nome são informações, porém cada uma delas tem uma relevância diferente para você. As informações mais sigilosas você esconde melhor e as menos sigilosas você não tenta esconder.



O que é informação?

Comunicação

A informação tem um importante papel nas relações entre diferentes indivíduos, sendo **fundamental para o processo de comunicação**. Existem diversas espécies que se comunicam com a transmissão das informações, às vezes como medidas de segurança, compartilhando informações sobre predadores, doenças ou lugares perigosos. A distinção dos seres humanos se faz pela **capacidade de codificar os dados formando assim a linguagem**.

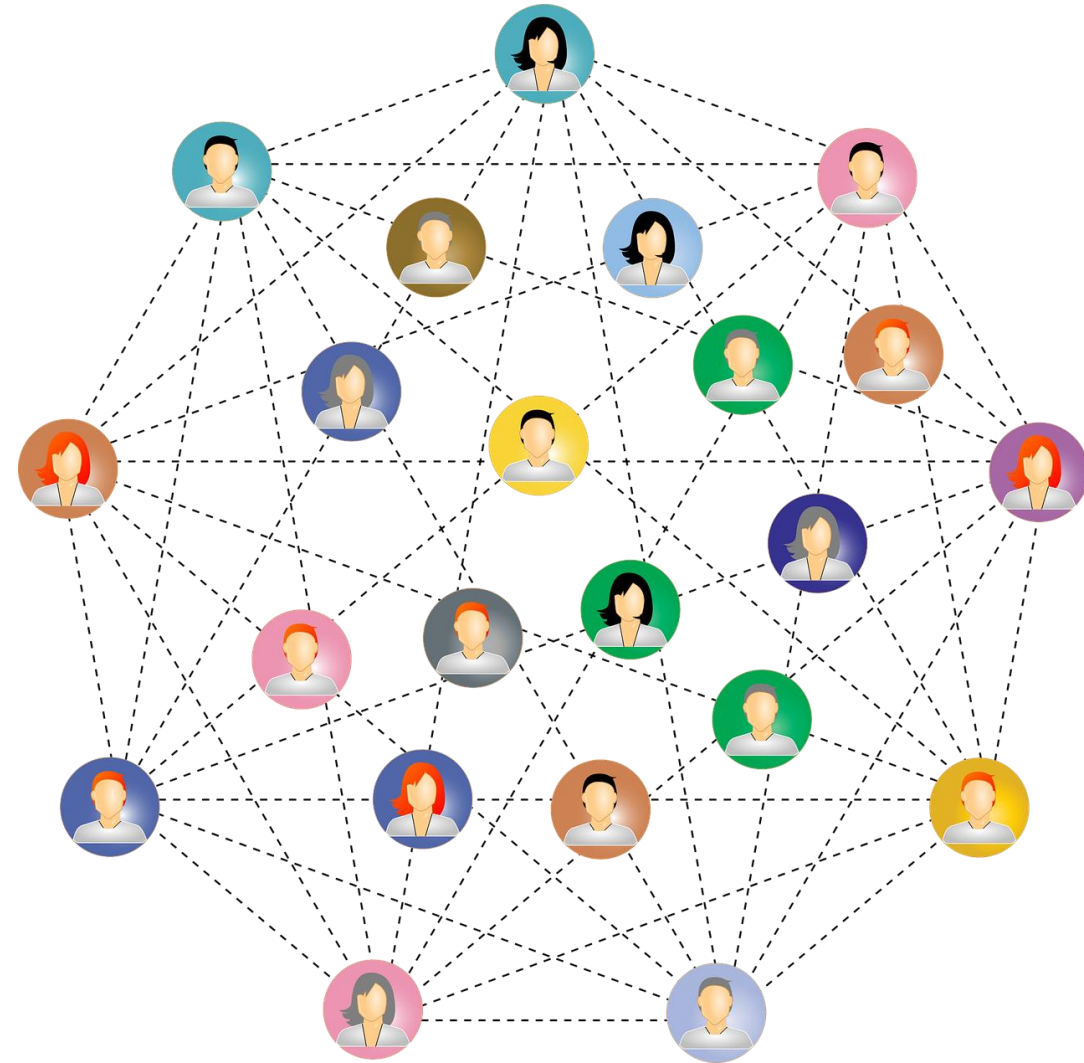


O que é informação?

Transferência do conhecimento

A informação não necessariamente é passada somente de uma pessoa para outra, ela **pode ser a transferência do conhecimento gerado em consequência da interpretação do conteúdo**. Ai você que estava entendendo tudo até agora, me pergunta. Como assim? Então para explicar melhor esse conceito devemos ter em mente que o **conhecimento é o ato de compreender por meio da razão então quando você**, por exemplo, ver uma imagem e você consegue compreender o que significa essa imagem você está gerando conhecimento, porque a imagem está te passando uma informação e você está absorvendo por meio da razão.

Nesse sentido **a informação é o conhecimento que está expresso na forma de escrita, oral ou audiovisual**.



Contexto histórico da informação

Ao longo da história, a forma de provimento à informação sofreu transformações, como poderemos observar na linha temporal abaixo.



Período Paleolítico

O acesso a informação era representado, através de **pictografias**, tais **pinturas rupestres**, nos interiores das cavernas, retratavam seu cotidiano representando suas conquistas e medos. Assim era uma forma de **transmitir a informação para as outras pessoas**, demonstrando quais eram os perigos enfrentados utilizando a informação como meio de alerta.

Idade Média

Informação era **concentrada nas bibliotecas e monastérios**, com **acessos restritos** a poucas pessoas, geralmente o acesso era somente para os membros da igreja.

Idade Moderna

Informação passou a ser **difundida**, pois com o **surgimento de meios de comunicação de massas**, como jornais, livros em série, rádios e a televisão. Estas ferramentas digitais facilitaram a dispersar as notícias e os acontecimentos. Na Idade Moderna as notícias começaram a ser transmitidas para um público maior e com mais velocidade.

Contexto histórico da informação

Antes de seguirmos com nossa viagem sobre a história da informação, vamos fazer uma breve pausa para entendermos melhor os acontecimentos ocorridos após a Segunda Guerra Mundial.



IMPORTANTE

Após a Segunda Guerra Mundial, no contexto da terceira revolução industrial, com o aparecimento de novas tecnologias, a fim de buscar o desenvolvimento industrial houve grandes transformações, como o desenvolvimento da robótica. Devido a essa necessidade de melhorar o processo de produção industrial e o processamento e o armazenamento de dados **surgiu a tecnologia da informação**.

O **processo de tratamento de informações** que antes era por meio de planilhas, artigos e memorandos, todos feitos através da datilografia e distribuídos por malotes, foi ficando cada vez mais obsoleto, pois a quantidade de informação estava crescendo e além dos documentos físicos ocuparem muito espaço eles eram difíceis de serem compartilhados. Imaginem só como na década de 60 uma pessoa iria enviar um documento dos Estados Unidos para o Brasil, demoravam dias até chegar, não precisamos nem ir tão longe um documento enviado internamente já demoravam dias.

Contexto histórico da informação



Décadas de 1960 e 1970


Em **1960**, os **computadores começaram a surgir** e foram aplicados nas empresas, além de serem raros ainda continham problemas quanto à aplicação e a compatibilidade entre si. Na **década de 70** com a permissão de acesso as linhas telefônicas **passaram a utilizar terminais remotos de computadores** onde as informações eram recebidas e processadas por um computador central que gerava relatórios e repassava para os computadores periféricos

Ainda com a necessidade de flexibilização, surgem os sistemas de informação e os softwares (programas) estimulando uma série de inovações.



Décadas de 1980 a 1990

Em **1980** começam o **surgimento dos microcomputadores** e a **expansão da tecnologia da informação** com o gerenciamento de banco de dados, onde mais pra frente **em 1990 aparecem os sistemas abertos** acabando com um dos maiores problemas que era a falta de compatibilidade.



Contexto histórico da informação

Após década de 1990

Com o **desenvolvimento da internet** transformaram ainda mais **acessíveis o compartilhamento de informações e armazenamento de dados**. Com um mundo globalizado há uma **quantidade enorme de informações** circulando entre as pessoas e com a velocidade com que elas são processadas, transmitidas e compartilhadas algo que ocorreu a milhares de quilômetros pode ser divulgado em questão de segundos.



IMPORTANTE

Dado o exposto no contexto histórico a **informação seguiu longos processos sem perder sua essência**, porém o que foi mudando foi a **forma como tratamos essa informação** e atualmente com os avanços tecnológicos um dos meios que se faz necessário para processar o número progressivo de informações é utilizando a tecnologia da informação.

O que é a Tecnologia da Informação (TI)?

É o conjunto de soluções para **promover a obtenção, o armazenamento, o acesso, o gerenciamento e o uso das informações**, por meios computacionais.

Uma importante questão abordada quando o assunto é TI é **como utilizar da melhor maneira as informações**. Na verdade tudo **depende dos fatores que te rodeiam** como cultura, mercado, ambiente e o próprio serviço. Saber como utilizar a TI é muito importante, pois assim não geram desperdícios.

A **TI pode ser um grande fator para empresas administrarem suas informações**, além de se tornarem mais competitivas no mercado sabendo valorizar suas informações e gerenciá-las. A proporção que a velocidade da informação se estabelece ela é acompanhada pela evolução do universo da computação e das novas tecnologias.

A informação com suas características tecnológicas trazem benefícios tanto em parâmetros **SOCIAIS** como **ECONÔMICOS**, que **aprenderemos um pouco mais a seguir**.



O que é a Tecnologia da Informação (TI)?



Parâmetro Econômico

É exposto como forma de **gestão da informação e suporte de decisões**, gerando um diferencial competitivo no mercado. Segundo McGee e Prusak (1994), em uma **economia de informação**, a **concorrência se baseia** em como a empresa **adquire, processa, interpreta e utiliza sua informação**.



IMPORTANTE

Por exemplo, pense em uma **empresa que atua no ramo de designer gráfico** e utiliza computadores com o melhor processador do mercado, porém com uma tela de monitor de 15 polegadas, com certeza os programas que fazem o designer gráfico vão rodar no computador, pois ele é o melhor do mercado, porém quando se trabalha com designer gráfico é necessário um monitor maior, por que um monitor com a área de visão menor dá mais trabalho para o funcionário que não consegue ver os detalhes do produto. Logo, reflete que a aquisição dos equipamentos interfere diretamente na produção, demonstrando que as decisões a serem tomadas na empresa devem ser passadas primeiramente pela área de TI.

O que é a Tecnologia da Informação (TI)?



Parâmetro Social

A importância da TI também pode ser apresentada em **questões quotidianas**. No nosso dia-a-dia estamos direta e indiretamente ligados a TI e sua utilização é bastante ampla.



IMPORTANTE

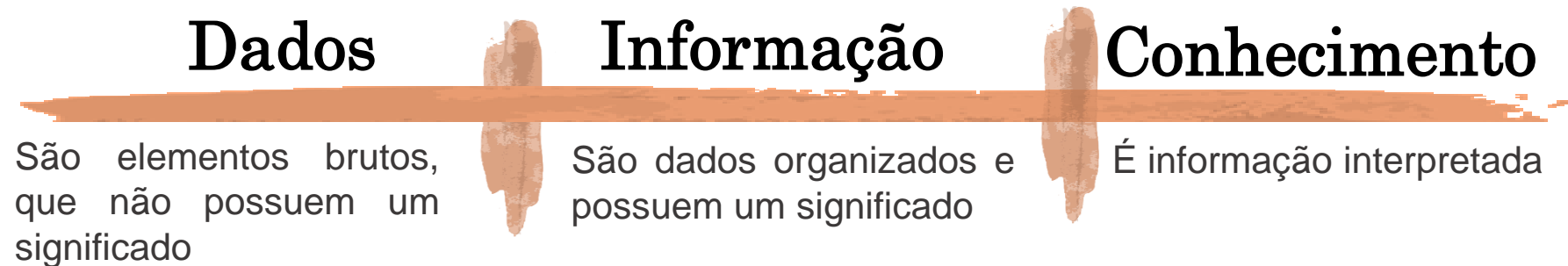
Por exemplo, o seu álbum de fotos, antes você tirava as suas fotografias, organizava e colocava no álbum de fotografias como forma de armazenamento. Hoje você pode armazenar suas fotos no seu computador e organizar de acordo com a data em que foi criado, o local em que foi retirado e assim organizar da forma que achar melhor.

O que é um sistema de informação?

Devido ao grande número de dados gerados com o decorrer do tempo **houve a necessidade de buscar meios para transformar esses dados em informações** e com isso **surgiram os sistemas de informação**.

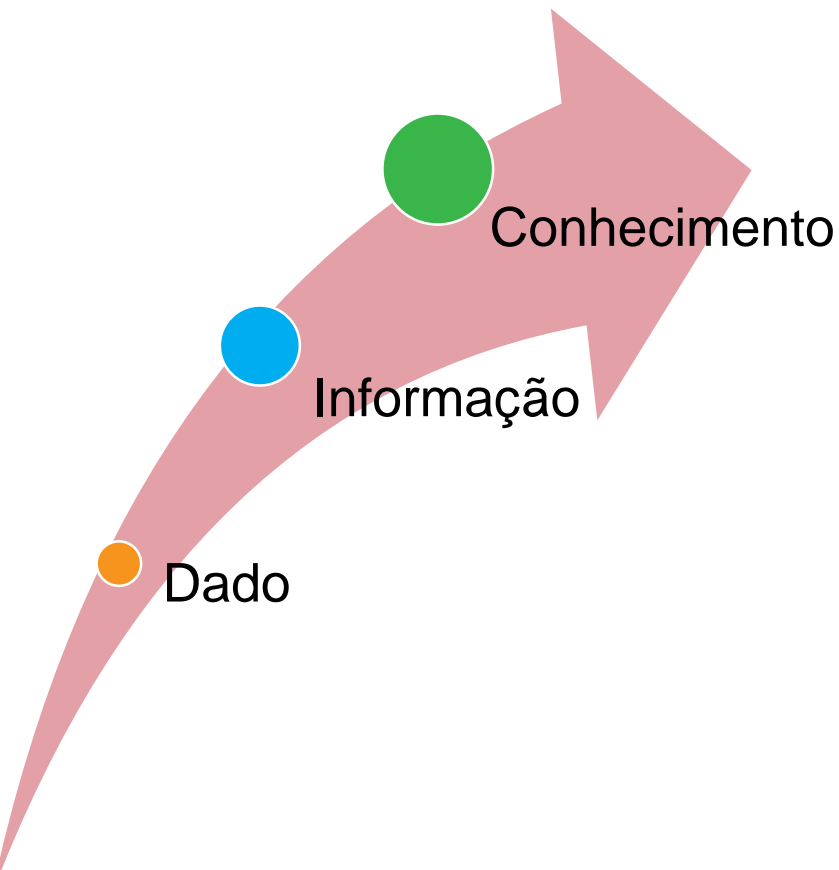
Em um sistema de informação nos devemos deixar bem claro os conceitos iniciais, lembrando que esses conceitos são em um viés técnico.

E quais são esses conceitos iniciais?



O que é um sistema de informação?

Conceitos iniciais



Podemos **pensar em dados**, dentro de uma empresa, como o salário do funcionário, pois o salário **sozinho não tem um significado para a empresa** é somente um número dentro de vários que a empresa contabiliza. Porém, **quando organizamos esses dados surge o conceito de informação**, por exemplo, a folha de pagamento dos funcionários então surgindo um significado e transformando aquele único dado em um conjunto de dados, ou seja, transformando em uma informação e **quando avaliamos os impactos** da folha salarial ou reavaliamos as faixas salariais **aparece o conceito de conhecimento**, pois a informação foi interpretada gerando um resultado maior.

Os **conceitos se interligam e dependem um do outro**, por que sem os dados que são a unidade inicial não teríamos o conjunto que é a informação e não teríamos a interpretação dos dados e só seriam conteúdos avulsos sem significado algum.

Para um **sistema bem organizado todos os conceitos devem está em sincronia** na falta deles atinge diretamente o posterior. Mas, o que é um sistema? Esse conceito aprenderemos melhor a seguir.

O que é um sistema de informação?

O que é um sistema?

É um **conjunto de partes que estão inter-relacionados e interdependentes**, essa integração de partes pode se dar por diversos meios, pode ser **fluxo de informações, matéria, energia**. Desse modo é a comunicação entre os componentes de um sistema.



IMPORTANTE

Só para deixar mais claro um **sistema não necessariamente será de informação ou computacional**, você pode encontrar vários tipos de sistemas como sistema ferroviário, sistema circulatório, sistema solar. Você mesmo tem um sistema que é seu sistema respiratório que é composto pela traqueia, brônquios e os pulmões que estão funcionando de forma independente, mas também de forma inter-relacionada para que você possa está respirando, pois se um para pode danificar o seu sistema respiratório.

O que é um sistema de informação?

Agora que já sabemos os dois conceitos separadamente (sistema e informação), podemos uni-los e apresentar o que seria um sistema de informação.

Um sistema de informação nada mais é que **um sistema que coleta dados que organiza, processa e distribui informações**, podendo ser automatizado, que seria um sistema de informação computadorizado. Exemplos de sistemas computadorizados são: **sistemas mais simples** como uma planilha de calculo ou um editor de textos; ou **mais complexos** como o MRP (*Material Requirement Planning*), que é um sistema computadorizado lógico de cálculo que converte a previsão da demanda em função da necessidade de seus componentes e o STP (Sistema de processamento de transações), que é um sistema de registro de transações e informações necessárias para o desenvolvimento de uma empresa.



O que é um sistema de informação?

Então, você já aprendeu os conceitos do sistema de informação, mas você deve está se perguntando, **qual seria a importância do sistema?** Ou mesmo, **por que uma empresa necessitaria de um sistema de informação?**

Para responder essas perguntas de uma forma simples, devemos ter em mente que um **sistema de informação pode ser utilizado para diversos fins**, como nas empresas de administração, contabilidade, engenharia entre outros; Indústrias alimentícias, automobilísticas, farmacêuticas etc. e no comercio de forma geral, tanto para controlar o estoque como verificar a demanda e a oferta de produtos. A seguir, vamos aprender sobre a importância de um sistema de informação.



O que é um sistema de informação?

Importância do sistema de informação



Um sistema de informação **auxilia nas conquistas das metas** organizacionais ou de negocio, **sintetizam os dados** das operações **facilitando a tomada de decisão**, **integram dados de fonte externa e interna** organizando o procedimento de dados e o surgimento de informações e **coletam, analisam , compartilham e monitoram a informação** oferecendo suporte na gestão de negócios. É importante frisar que um banco de dados sem está organizado não gera informação, com isso formando apenas dados sem significados, assim servindo apenas para ocupar espaço.

O que é um sistema de informação?



IMPORTANTE

Para melhor entender, pense em um comércio de atacado, vamos chamá-lo de Comércio Y. O Comércio Y atua na área de materiais para papelaria e no seu estoque tem vários produtos como cadernos, livros, borracha, caneta, lápis e outros materiais. Imaginemos que esse comércio não possui um sistema de informações, seria uma bagunça, pois ele não saberia quantos cadernos ele teria, por quanto ele comprou cada caderno, qual a diferença entre os cadernos.

Então essas informações, que são de suma importância para o gerenciamento do negócio, devem ser processadas para que fique claro a quantidade de materiais no estoque e não venda mais do que tem ou quantos materiais precisam ser comprados para evitar a falta no estoque. Relembrando que não necessariamente um sistema deve ser computadorizado, ele também pode ser manual. Claro vai dar mais trabalho e pode ser que perca a organização de acordo com o crescimento da empresa, por isso é recomendável um sistema informatizado com ferramentas adequadas. Também vale lembrar que o sistema não é somente para o negócio, mas também para diversos tipos de funcionalidades.

O que é um sistema de informação?

O sistema de informação **pode ser dividido em quatro** partes principais:

- » **Entrada (*input*)**: envolve a captação de dados brutos do ambiente interno e externo;
- » **Processamento**: compreende o tratamento e organização dos dados brutos;
- » **Saída (*output*)**: consiste no resultado dos dados processados e organizados e na transferência para o usuário final ; e
- » **Retroalimentação (*feedback*)**: envolve o retorno da informação que serve para avaliar os resultados do fluxo, podendo ser positivo ou negativo, assim ajudando o sistema a melhorar continuamente.



Segurança da informação

Agora que já vimos os conceitos de Informação e Tecnologia da Informação (TI), estamos preparados para iniciar o conteúdo de segurança da informação.

A preocupação com a segurança da informação não é um assunto novo, já que tudo que tenha certa importância, como é o caso da informação, se busca proteger. Assim para começar a falar sobre a segurança da informação dentro da tecnologia da informação, podemos entender melhor o contexto histórico da segurança da informação.

Por volta de 600 anos a.C.

Com o intuito de **proteger seus escritos, surgiu às cifras hebraicas**. Com o objetivo de evitar que leem-se seus textos, os hebreus criaram um tipo de criptografia, baseada em um sistema de substituição simples, ou seja, a primeira letra do alfabeto é trocada pela última, a segunda letra pela penúltima e assim sucessivamente.

Na idade média

Com a intenção de **evitar roubos dos livros**, que poderiam valer fortunas, as **bibliotecas acorrentavam os livros**. Contudo, esses meios foram evoluindo assim com a forma de gerenciamento das informações.

Atualmente

Esses meios de proteção foram evoluindo assim com a forma de gerenciamento das informações. Atualmente, com a velocidade em que a tecnologia se move, é **necessário está atento às novas ameaças e sempre buscar maneiras de combatê-las** e abreviar os danos causados.

Segurança da informação

Com a crescente **importância das informações**, as mesmas são **consideradas um ativo** muito importante para as organizações. Esses ativos, que são intangíveis, é **um dos maiores patrimônios das organizações modernas** e sendo **vital para a instituição**, devem ser **protegidas e gerenciadas** com eficiência.

No contexto atual, a **segurança da informação age de forma a proteger os sistemas, dados e informações valiosas**. A fim de evitar perdas ou roubos em que constituiriam um prejuízo para as organizações.



Segurança da informação

Crimes virtuais

De acordo com a estimativa da Cyberventures, consultoria internacional na área de segurança na Internet, os **prejuízos causados com ataques cibernéticos** em parâmetro mundial é de **mais US\$ 5 bilhões em 2016**. A consultoria prevê que **os crimes cibernéticos custem ao mundo US\$ 6 trilhões até 2021**.

Casos de **crimes virtuais têm ocorrido de forma frequente atingindo geralmente empresas de pequeno e médio porte**, pois, devido à falta de investimentos em sistemas de segurança da informação, acabam sendo alvos fáceis. Assim como afirma André Miceli, professor do MBA de Marketing Digital da Fundação Getúlio Vargas (FGV).

“As grandes empresas já dedicam uma parcela de seus orçamentos de tecnologia para segurança. Isso ainda não acontece nas pequenas e médias. Assim como no mundo ‘físico’, os criminosos procuram facilidade, então essas empresas acabam caindo nessa situação com mais frequência”.



IMPORTANTE

Segundo a empresa Norton Symantec Corporation, em seu relatório “2016 Norton Cyber Security Insights Report”.



39% dos americanos sofreram, pessoalmente, o cibercrime no ano passado. No mundo esse da é de 31% das pessoas.



A Holanda tem a **taxa mais baixa de cibercrime** experimentada no último ano (**14%**), em comparação com a Indonésia com a maior taxa (59 %).



No Brasil, o cibercrime girou mais de **R\$ 32 bilhões em 2016**.

Os dados dos crimes virtuais têm aumentado conseqüentemente e com isso devemos está atentos à segurança da informação para tentar evitar fraudes e prejuízos.

Segurança da informação

Crimes virtuais

O nível de proteção é estabelecido de acordo com o valor e os seus potenciais danos. Vale ressaltar que a segurança não está ligada somente a combater as ameaças, mas também pelos procedimentos e comportamentos para evitar vulnerabilidades e se prevenir dos ataques.

Alguns países como Alemanha e Estados Unidos, Reino Unido já possuem uma cultura maior voltada para a prevenção, todavia o ISTR, volume 22 (Relatório de ameaças à segurança na internet de 2017) oferecido pela Norton Symantec Corporation, demonstra que mesmo assim **metade das empresas ainda está mal preparada** para lidar com ataques cibernéticos.

Não basta apenas combater as ameaças digitais devemos **aprender comportamentos para evitar** que os ataques cheguem e causem algum dano, de modo a se prevenir e se preparar melhor das ameaças. É necessário ter consciência que **não existe segurança perfeita, total ou absoluta**, o que **devemos alcançar é a segurança satisfatória**. A segurança satisfatória é aquela que busca minimizar e/ou neutralizar as possibilidades de agressão.



SAIBA MAIS

Para saber mais acesse: http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf

Tema 2

Princípios e conceitos da segurança da informação

Olá! Vamos ao Tema 2 e nesta etapa serão apresentados os **princípios** referentes à segurança da informação, assim como importantes **conceitos** que o auxiliaram no estudo do assunto como: vulnerabilidade, ataque e atacantes, entre outros.



Princípios da segurança da informação

A segurança da informação aparece com o intuito de assegurar a proteção das informações de vulnerabilidades e preservar o valor que possuem para um indivíduo ou organização. Segundo o Prof. André Alencar dos Santos,

“A segurança da informação tem por objetivo proteger a informação de diversos tipos de vulnerabilidade (possibilidade de **perda de algum dos pilares da segurança da informação**) e, também quando houver a concretização da ameaça (ataque), procura estabelecer um plano de continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e das oportunidades”.

A segurança da informação é constantemente desafiada a cumprir seus pilares, onde, geralmente, nos problemas enfrentados eles são referência.



SAIBA MAIS

Quais são os **Pilares da segurança da informação**?

Também chamados de princípios, são três os conceitos que formam a base para os objetivos da segurança da informação em todos os sistemas:



Princípios da segurança da informação

■ Princípio da Confiabilidade

Garante que a informação somente seja acessada por pessoas autorizadas, tendo como relação o **sigilo da informação**. Como forma de garantir a confidencialidade são utilizados controles de acessos, que protegem a informação contra a divulgação não permitida, como: a autenticação por senha e a permissão de utilização. Esse conceito é bastante interessante, pois **no mundo corporativo devemos privar pelo sigilo e proteger o capital intelectual** devido às consequências de vantagens competitivas.

Imagine que você é sócio de uma empresa e vai lançar um novo produto no mercado, mas antes você precisa validar com seu sócio. As únicas pessoas autorizadas a ver o produto é você e seu sócio, então você envia o produto por e-mail para ele. Contudo seu concorrente, que está interessado nesse novo produto, consegue capturar o e-mail e lê o conteúdo. Nesse caso, feriu o conceito de confidencialidade, pois uma pessoa não autorizada, seu concorrente, conseguiu ter acesso ao conteúdo.



Princípios da segurança da informação



SAIBA MAIS

Para garantir a segurança da informação de qualquer empresa, é **necessário que haja normas e procedimentos claros**. A ISO/IEC 27002 é a norma internacional de gestão de segurança, que aponta atributos básicos e estabelece diretrizes e princípios gerais para a iniciação, implementação, manutenção e a melhoria da gestão de segurança da informação.

Princípios da segurança da informação

■ Princípio da Disponibilidade

Permite que a informação esteja disponível para acesso no momento desejado, não só para o cliente mas, também, para a organização garantindo a continuidade do serviço. A **disponibilidade está intrinsecamente contida na eficácia do sistema** e no seu correto funcionamento. A maneira para assegurar a disponibilidade pode ser apresentada por meio de *backups*.

Por exemplo, você trabalha em um banco e frequentemente atende telefonemas, pois os clientes do banco querem saber a situação financeira deles como: se eles têm limites para pegar um empréstimo, quanto eles possuem na poupança, etc. Você deve verificar no sistema para obter essas informações. Todavia em uma dessas ligações, quando você foi acessar o sistema, estava fora do ar, devido a problemas relacionados a estabilidade. Logo, afetou o princípio da disponibilidade, já que no momento em que foi necessário, o sistema ele não estava funcionando.



Princípios da segurança da informação

Princípio da Integridade

Assegura que a informação não seja alterada por pessoas não autorizadas, garantindo a inteireza da informação de modo que saia da origem e chegue ao destino sem ser violada ou modificada, mantendo os dados íntegros e inalterados no seu transcurso. Utiliza-se a criptografia como meio para alcançar a integridade.

A integridade pode ser observada na mesma situação do caso da disponibilidade, só que quando seu concorrente consegue interceptar o e-mail ao invés de apenas lê, ele altera as informações do produto. Supondo que o produto era uma caneta vermelha, então muda a cor da caneta de vermelha para azul e envia seu e-mail para seu sócio. Atingindo o princípio da integridade, pois o conteúdo do e-mail foi alterado por uma pessoa não autorizada violando sua integridade.



Princípios da segurança da informação

Outros Princípios

Autenticidade

Garante a identidade de quem está enviando a informação, através do qual garante que a informação é procedente da fonte anunciada. Um dos mecanismos que compreende o princípio é o da assinatura eletrônica.

Não Repúdio ou irretratabilidade

Visa **garantir que o autor não negue a criação de algum documento** ou a sua assinatura, não podendo se esquivar da sua autoria.

Privacidade

Determina quais informações estarão disponíveis e para quem. Os princípios da confidencialidade e da autenticidade são utilizados como meios para conseguir a privacidade.

Legalidade

Uso da tecnologia da informação de forma a seguir as leis vigentes do local ou país.

Princípios da segurança da informação



IMPORTANTE

Estes princípios são tão importantes quanto os três pilares da segurança da informação, sendo sua compreensão crucial para a Política de Segurança da Informação, permitindo que se determinem os meios adequados para manter o sistema confiável e organizado.

Conceitos importantes no estudo da Segurança da Informação



Depois de apresentarmos os princípios da segurança da informação é necessário conhecer alguns conceitos importantes sobre o tema. Então, nesta etapa, aprenderemos sobre os seguintes conceitos:

- Vulnerabilidade (Hardware, Comunicação, Humana e de Armazenamento)
- Ameaça
- Ataques
- Atacantes (Hackers, Crackers)
- Intrusos (Passivos e Ativos)
- Conceitos Avaliativos (Conformidade, Credibilidade, Efetividade e Eficiência)

Vulnerabilidade

São falhas que comprometem o sistema atingindo os pilares da Segurança da Informação. São divididas em quatro principais tipos:

- 1 Vulnerabilidades de **Hardware**.
- 2 Vulnerabilidades de **Comunicação**.
- 3 Vulnerabilidades de **Armazenamento**.
- 4 Vulnerabilidades **Humanas**.



Vulnerabilidade

1

Vulnerabilidades de **Hardware**

São equipamentos de hardware que por serem mal instalados ou desenvolvidos acabam se apresentando com maior facilidade para vários tipos de ataques. Os ataques que ocorrem em equipamentos de hardware ocorrem por conta da má instalação, drives desatualizados. Os *modems* são os hardwares, geralmente, mais acessíveis para um ataque malicioso, já que os atacantes aproveitam do uso de senhas fracas ou padronizadas para acessarem os painéis de controle do dispositivo.



Vulnerabilidade

2

Vulnerabilidades de **Comunicação**

Consiste em quando as redes privadas são acessadas sem o devido cuidado ou quando alguém com habilidades técnicas avançadas conseguem invadir a rede privada e capturar informações. As redes privadas são onde ocorrem a troca e visualização de pacotes de dados, quando alguém explora essas vulnerabilidades, acaba atingindo o princípio da confidencialidade e também pode atingir o da integridade.



Vulnerabilidade

3

Vulnerabilidades de **Armazenamento**

São as que afetam dispositivos de armazenamento como: HDs externos; pen drives; SDDs (*SolidState Drive*), que são os “cartões de memória” de máquinas e celulares, entre outros. Essa vulnerabilidade pode ser explorada por ataques simples como vírus de script, podendo assim apagar todas as informações.



Vulnerabilidade

4

Vulnerabilidades **Humanas**

Dentre as apresentadas, estas são as mais comuns, pois é a ação feita pelo próprio usuário que compromete a segurança, dando chances para que vários ataques aconteçam. É a vulnerabilidade mais perigosa. Devido a falta de treinamento essa vulnerabilidade acaba ocorrendo com frequência. São formas que representam essa vulnerabilidade: o *download* de aplicações inseguras, senhas simples e a repetição para vários sistemas diferentes, o acesso a conteúdos maliciosos, entre outros.



Ameaça

É a ação praticada por *softwares* com intenções maliciosas, quando exploram as vulnerabilidades do sistema e obtém êxito. Exemplos de ameaças são: os *malwares* e os *scan's* que serão vistos no tema 3.



Ataque

Consiste na concretização da ameaça.

Podem ser:

- acidentais ou intencionais;
- internos ou externos.

Acidentais

Consiste em quando um usuário, sem intenção de causar prejuízos, por imprudência, imperícia ou negligência acaba causando danos que atingem os pilares da informação. Por exemplo, imagine a seguinte situação: um funcionário de uma empresa recebeu um e-mail, este e-mail informava que ele foi sorteado e que ele iria ganhar um carro, devendo abrir o arquivo que estava anexo e executá-lo em sua máquina, sem pensar que aquilo poderia danificar sua máquina, o funcionário executa o arquivo e o seu computador é infectado.

Intencionais

Os ataques intencionais partem de usuários legítimos ou não da instituição, a fim de danificar as informações ou ter acesso às mesmas.

Por exemplo, o funcionário da empresa X aceita uma vantagem indevida da empresa Y, concorrente da empresa X. O funcionário deve colocar um vírus nas máquinas da empresa X.

Ataque

Internos

Ataques intencionais se dão de usuários legítimos, ou seja, internos ao ambiente, que tem o propósito de causar dano e utilizam do seu acesso aos recursos tecnológicos para cumprir com seus objetivos. Por exemplo, um funcionário da empresa insatisfeito por ter pedido o aumento e não ter recebido, decidiu atingir a empresa de alguma forma. Para isso, utilizou um *pendrive* pessoal contendo vírus de computador e executou o arquivo malicioso na máquina da empresa. Esse vírus atacou o computador e excluiu todos os arquivos importantes.

Externos

Partem de usuários não autorizados que utilizam de meios fraudulentos, como golpes ou exploram as vulnerabilidades do sistema, para obter informações ou causarem danos. Por exemplo, um hacker que deseja roubar informações privilegiadas de uma determinada empresa para que possa vendê-las a uma empresa concorrente.

Ataque

Como foi possível observar, os ataques são divididos em quatro subcategorias e estas subcategorias podem se completar. Podemos ter ataques que são acidentais internos, acidentais externos, intencionais internos, intencionais externos.



IMPORTANTE

Exemplo 1: Supondo que um funcionário de uma empresa desejava escutar uma lista de músicas no seu trabalho, então ele trouxe de casa um CD MP3 com várias músicas do seu gosto. Contudo, ele não sabia que o CD continha vírus de computador, assim quando ele colocou o CD no computador os vírus se espalharam e atacaram as planilhas de cálculos da empresa, deletando-as. Em qual das categorias se encaixaria essa situação?

- Se você respondeu acidental interna, então você acertou. Porque nessa situação o funcionário da empresa não tinha a intenção de danificar o sistema, pois ele não sabia que o CD continha vírus e foi interna por conta de ser um indivíduo que faz parte da empresa e utilizou do seu acesso aos recursos tecnológicos.

Ataque

Como foi possível observar, os ataques são divididos em quatro subcategorias e estas subcategorias podem se completar. Podemos ter ataques que são acidentais internos, acidentais externos, intencionais internos, intencionais externos.



IMPORTANTE

Exemplo 2: X é funcionário de uma empresa e Y é amigo de X e não é funcionário da empresa em que X trabalha. Certo dia, Y enviou um e-mail para X informando que naquele e-mail estava em anexo um arquivo que continha fotos de quando os dois eram criança e que o arquivo não continha vírus de computador, contudo Y sabia que o arquivo continha vírus, pois sua intenção era roubar informações da empresa. X recebeu o arquivo e executou em seu computador. Com a execução do arquivo o vírus se espalhou pelo computador e roubou informações. A qual categoria esse caso poderia se adequar?

- Temos duas categorias. A primeira situação acontece quando X tendo acesso aos recursos tecnológicos da empresa, por ser funcionário e sem intenção de causar dano acaba espalhando o vírus e a segunda situação acontece quando Y que não participa da empresa e não é autorizado a acessar os recursos tecnológicos da mesma consegue roubar as informações. Ocorrendo respectivamente, acidental interna e intencional externa.

Atacantes

São pessoas que iniciam uma ação ofensiva, ou seja, pessoas que utilizam suas habilidades técnicas para acessar sem autorização os recursos informáticos de terceiros, explorando as vulnerabilidades do sistema ou humanas.

Podemos classificar os atacantes em:



Hacker



Cracker

Atacantes

Hacker

São usuários com profundo conhecimento em programação e informática que se dedicam intensamente a conhecer e modificar os aspectos de dispositivos, programas e redes. O Hacker busca falhas de segurança, a fim de explorá-las e tentando exceder o funcionamento normal do sistema e contornar barreiras utilizadas para impedir o acesso. Eles normalmente compartilham informações com o propósito de colaborarem com a comunidade sobre erros nos sistemas, falhas de segurança, criação de softwares livres. São responsáveis por diversas inovações que ocorreram no contexto da informática. Alguns hackers são contratados para trabalharem em empresas e órgãos governamentais onde testam a segurança dos sistemas descobrindo sua fragilidade e melhorando para prevenir ataques futuros.



SAIBA MAIS

Você sabia que podemos apresentar como exemplo de um hacker, Alan Cox. Cox é um programador britânico que mantém a árvore 2.2 do Cerne Linux. O Linux é um software livre de código fonte aberto, o que Cox fez foi estudar o código fonte do Linux e tentar melhorá-lo, revelando diversos problemas no código de rede, corrigindo vários deles e reescrevendo o subsistema de rede, ajudando assim a eficiência do sistema.

Atacantes

Cracker

São usuários com profundo conhecimento em programação e informática, que exploram as vulnerabilidades, tentando quebrar códigos de segurança e invadir sistemas. Porém, os crackers usam seu conhecimento para fins ilegais ou prejudiciais se dedicando a danificar dados, excluí-los ou roubá-los.

Existem alguns tipos de cracker, que são:

- **Cracker de criptografia:** pessoas que agem para quebrar criptografia e roubar informações.
- **Cracker de softwares:** pessoas que alteram o funcionamento de um programa para utilizá-lo para fins ilícitos.
- **Desenvolvedores de malwares:** pessoas que desenvolvem pragas virtuais, a fim de espalhá-las e causar prejuízos a terceiros.

Atacantes



Hackers e Crackers possuem propósitos diferentes.

Enquanto hackers visam melhorar os sistemas informáticos apontando falhas e vulnerabilidades, os crackers buscam roubar informações, destruir dados e causar prejuízos procurando lucrar com a possível ação.

Hackers apesar de invadirem sistemas, os mesmos promovem conhecimento e auxílio a terceiros e não a destruição de trabalho alheio e a comercialização de informações.

Atacantes



Hacker



Cracker

Vale ressaltar a diferença entre os Hackers e os Crackers. É muito comum que pessoas leigas generalizem os termos, pensam que Hacker é uma pessoa maliciosa responsável por invadir computadores e roubar informações, porém é importante deixar claro que há diferença entre as duas terminologias.

Assim como afirma a TMRC (Tech Model Railroad Club):

“Nós aqui no TMRC usamos o termo 'hacker' só com o seu significado original, de alguém que aplica o seu engenho para conseguir um resultado inteligente, o que é chamado de 'hack'. Ele atinge os seus objetivos sem modificar o projeto total do sistema. Apesar de não se encaixar no 'design' geral do sistema, um 'hack' é, em geral, rápido, esperto e eficiente. O significado inicial e benigno se diferencia do significado recente - e mais utilizado - da palavra 'hacker', como a pessoa que invade redes de computadores, geralmente com a intenção de roubar ou vandalizar. Aqui no TMRC, onde as palavras 'hack' e 'hacker' foram criadas, e são usadas com orgulho desde a década de 1950, ficamos ofendidos com seu uso indevido para descrever atos ilegais. Pessoas que cometem tais coisas são mais bem descritas por expressões como "ladrões", "cracker de senhas" ou "vândalos de computadores". Eles, com certeza, não são verdadeiros 'hackers', já que não entendem os valores 'hacker'. Não há nada de errado com o 'hacking' ou em ser um 'hacker'.”

Atacantes

Existem ainda outros tipos de atacantes, que se tomam de base à classificação de hackers e crackers.

- **Defacer:** são usuários responsáveis por modificar, danificar ou desfigurar a superfície ou aparência de um site da internet, programas de computadores, entre outros. Os defacers são conhecidos como “pichadores virtuais”, pois eles invadem um site, por exemplo, e deixam mensagens ou assinaturas para serem reconhecidos em grupos da internet. Esses ataques geralmente são de cunho pessoal, mostrando assim que ele foi capaz de invadir.
- **Phreaker:** estão mais focados em atacar sistemas telefônicos e sinais de TV a cabo. Utilizando indevidamente linhas telefônicas.
- **Caders:** são especialistas em roubar dados bancários e financeiros, como dados de cartões de crédito, senhas de banking, informações de cadastros de lojas para utilizar em outras compras online, etc.



SAIBA MAIS

Para saber mais sobre o assunto acesse:

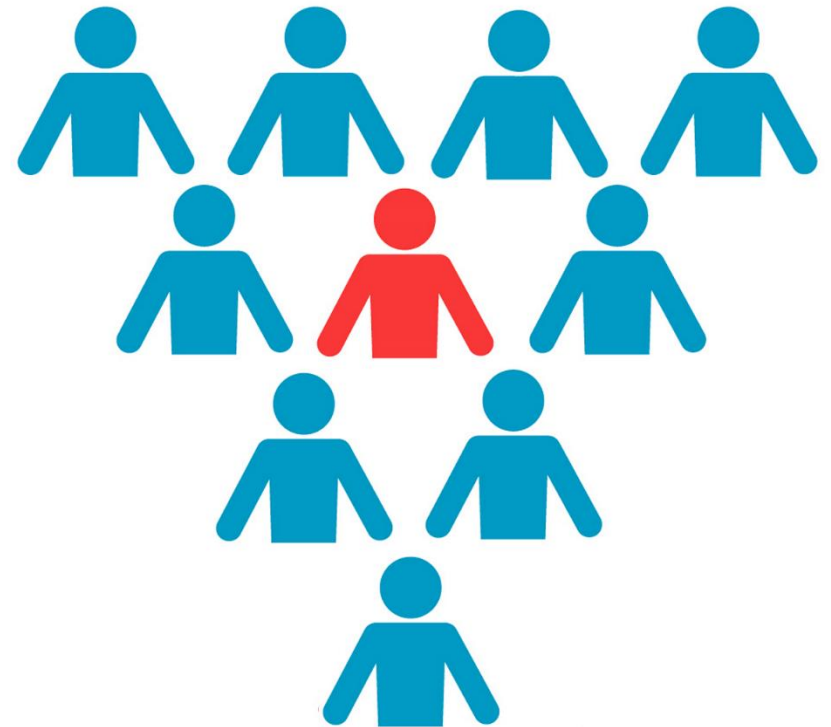
<https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-en.pdf>

Intrusos

O conceito de intrusos se assemelha bastante com o de atacantes.

Os intrusos são divididos em:

- **Intrusos passivos:** são os que entram no sistema com a intenção de espionar, assim ele entram no sistema e observam as informações, mas não destroem os dados.
- **Intrusos ativos:** são os que entram no sistema com o objetivo de além de obter informações também visam destruí-las .



Conceitos Avaliativos

São os conceitos para avaliar a competitividade do sistema de informação junto com a sua segurança.

As concepções apresentadas são as seguintes:

- **Conformidade:** similar ao princípio da legalidade, diz respeito a conformidade com os atendimentos legais no processo de segurança da informação, respeitando às normas da organização.
- **Credibilidade:** característica de confiança no sistema, fornecendo informações corretas, precisas e confiáveis para o usuário. A credibilidade é construída com a observância da conformidade e da eficiência.
- **Efetividade:** refere-se à capacidade de produzir o seu efeito habitual com constância e atingindo o seu objetivo real, atendendo de forma precisa e pontual, ou seja, quanto mais efetivo um sistema é mais credibilidade ele tem.
- **Eficiência:** capacidade de conseguir o melhor rendimento possível com o mínimo de erros, respeitando o princípio da economicidade.

Conceitos Avaliativos



IMPORTANTE

Um sistema que respeita todos os conceitos apresentados ganha força e competitividade no mercado. Deste modo alinhado com a segurança da informação os sistemas são capazes de responder as demandas e apresentar um bom rendimento, evitando assim futuros ataques.



SAIBA MAIS

[Para saber mais assista o vídeo:](#)



Tema 3

Gestão de processos de segurança



Parabéns, chegamos ao último tema e falta pouco para concluirmos nossa jornada. Então vamos lá! Nesta etapa serão exibidas algumas das **formas de gestão no processo de segurança da informação**.

Para isso, apresentaremos temas referentes as ferramentas que auxiliam na segurança da informação como a elaboração de políticas de segurança e análise de riscos.

Análise de Riscos na Segurança da Informação

A análise de riscos consiste em uma ferramenta capaz de identificar os possíveis riscos presentes no ambiente informático, determinando a frequência dos eventos ocorridos e a magnitude de suas consequências.

Na área da segurança da informação, a análise de risco, tem como objetivo **identificar os riscos e mensurar os possíveis danos que podem causar ao ambiente**, deste modo servindo de parâmetros para justificar os controles de segurança além de mapear as áreas de risco do sistema e apresentar medidas eficazes para o combate nas áreas especificadas, diminuindo os erros e maximizando a eficácia dos sistemas.

A análise de risco é fundamental para a segurança da informação, pois ambos os conceitos encontram-se intimamente ligado e determinam os aspectos de controle da segurança, de acordo com a necessidade do atendimento da Confidencialidade, Integridade e Disponibilidade (pilares).

Análise de Riscos na Segurança da Informação



IMPORTANTE

Segundo Robert N. Charette “a análise de riscos não diz respeito a decisões futuras e sim o futuro de decisões presentes”.

Com uma **análise de risco competente podemos aumentar a probabilidade de sucesso** no ambiente da tecnologia da informação, possibilitando: melhores resultados e diminuindo as surpresas; além de alinhar os objetivos de segurança com os requisitos do negócio; e adequando o valor do orçamento com o custo a ser aplicado em questões de segurança. Este ultimo benefício é muito importante realçarmos, pois é necessário que a empresa saiba o valor do seu ativo intangível que são as informações adequando o custo de perdê-las e o valor aplicado em investimentos na segurança delas.

Análise de Riscos na Segurança da Informação

O que é um risco?

Risco está **associado à exploração de uma ou mais vulnerabilidades do sistema**, por meio de ameaças, que impactam negativamente os recursos tecnológicos e a atividade da organização. O risco está diretamente ligado à incerteza. Logo quando você conhece os riscos você evita que eles aconteçam. O risco é composto por quatro critérios, que são:



Causa Raiz: que é a origem do risco, ou seja, é o acontecimento.



Efeito: é a consequência produzida por uma causa raiz.



Probabilidade: são as chances de que o evento venha ocorrer.



Impacto: É o resultado que ocorre caso o evento ocorra.

Análise de Riscos na Segurança da Informação



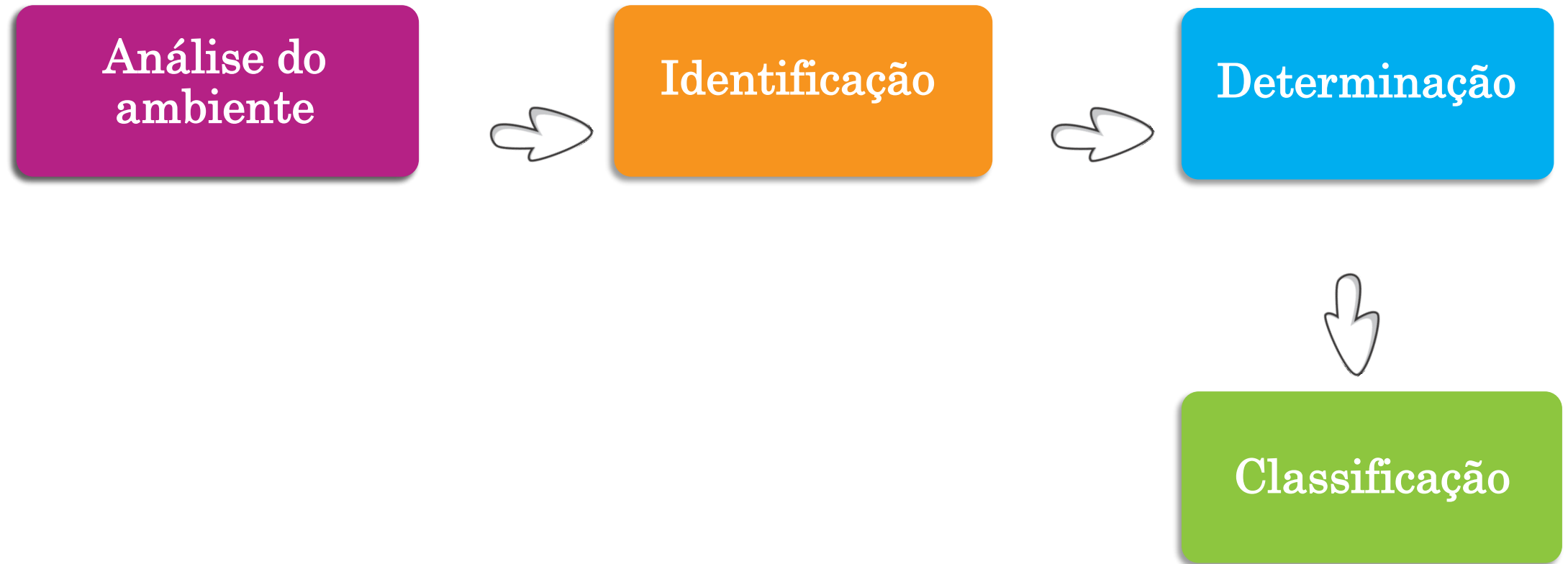
IMPORTANTE

Exemplo: supondo que você fez um trabalho e deixou esse arquivo salvo no computador, porém você não fez cópias de segurança e antes de você desligar você percebeu que ele estava aquecendo. No dia seguinte seu computador queimou e você perdeu o arquivo. A **causa raiz foi não ter feito a cópia de segurança**, pois assim você estava à mercê do risco; **o efeito foi o fato de perder o trabalho**; a **probabilidade são as chances do seu computador queimar** que eram altas, pois você tinha sentido que o computador estava aquecendo; e **o impacto foi o sentimento de não ter sido produtivo** já que tudo que você fez você perdeu, ou seja, você ter ficado sem seu trabalho. Assim pode-se concluir que a causa raiz está ligada à probabilidade e o efeito ao impacto do evento, então $\text{exposição ao risco} = \text{probabilidade} \times \text{o impacto}$.

Análise de Riscos na Segurança da Informação

Etapas da análise de risco

Após entendermos o que é um risco e como funcionam seus componentes. Devemos começar a realizar as etapas da análise de risco, a seguir descritos:



Análise de Riscos na Segurança da Informação

Etapas da análise de risco

Análise do ambiente

Deve-se verificar o estágio de maturidade da empresa (ambiente interno), mapeando: o grau de vulnerabilidade existente; a probabilidade da ocorrência de um incidente de segurança; as consequências do cálculo dos riscos associados. Após o mapeamento do ambiente interno, precisamos nos atentar ao ambiente externo, pois as mudanças tecnológicas ocorrem com muita velocidade e devido a isso as organizações devem manter esforços para monitorar quaisquer alterações externas.



Análise de Riscos na Segurança da Informação

Etapas da análise de risco

Identificação

Devemos **identificar dois fatores**: os recursos considerados críticos (nível crítico) e as vulnerabilidades e ameaças associadas aos recursos. Vamos lá?

Nível crítico de algo é **definido**: a) **pela sua relevância para o negócio**, logo se um dado for muito importante para a empresa seu nível crítico é maior, por exemplo, um banco de dados contendo todas as informações dos clientes é de extrema importância para a empresa com isso seu nível crítico vai ser valorizado; b) **pela facilidade de substituição**, caso algo seja de fácil substituição ele não terá um nível crítico alto, pensa comigo, se eu tenho um site que eu sempre leio notícias e de repente esse site “sai do ar” ou para de funcionar, eu facilmente posso substituí-lo por outras centenas de sites que também fornecem notícias; e pelo **investimento necessário para reparação ou substituição**, quando o custo operacional ultrapassa as vantagens oferecidas o nível crítico também diminui.

Vulnerabilidades: após a identificação dos recursos críticos para o sistema teremos indicadores que auxiliaram a definir as prioridades (os recursos mais críticos do nosso sistema podem ser: banco de dados dos funcionários ou dos clientes, documentos digitalizados, entre outros), identificando quais são suas vulnerabilidades e as ameaças e também a probabilidade de ocorrências de ataques.

Análise de Riscos na Segurança da Informação

Etapas da análise de risco

Determinação

Deve-se estabelecer o valor dos recursos (tangíveis e intangíveis), inclusive os valores indiretos, e associarmos aos impactos resultantes da concretização de uma ameaça sobre o recurso. Deste cálculo surge o nível de risco.


Vamos deixar esse conceito mais claro! Esses recursos que foram identificados possuem um valor para a organização, então nessa etapa devemos determinar qual é esse valor. Com isso, os custos com a segurança desse recurso não podem ser maior que o seu próprio valor.

Vamos tomar como exemplo algo mais tangível, para ficar mais claro. Você tem uma carga de laranjas para você calcular o nível de risco dessa carga você tem que saber quanto ela custa. Vamos supor que a carga custe R\$ 5 mil e só de lucro líquido você consegue R\$ 3 mil, onde você guarda a carga acontecem muitos assaltos e um seguro contra roubos custa R\$ 300. Então pelo seu nível de risco compensa você não aceitar risco e contratar um seguro. No final das contas você ainda vai ganhar R\$ 2.700.

Análise de Riscos na Segurança da Informação

Etapas da análise de risco

Classificação



Deve-se interpretar o nível de risco e, de acordo com o que foi identificado, acontece à aceitação ou a necessidade de ajustes. Quando uma organização não aceita o nível de risco que dizer que as consequências são significativas para a concretização das suas atividades críticas. Em outras palavras, a instituição decidiu em não correr riscos, pois caso eles aconteçam os impactos podem ser maiores que o custo de evitá-los. Porém, quando a organização aceita o nível de risco ela conclui que as consequências que podem ser geradas não são significativas para as suas atividades, porém apesar da empresa aceitar o nível de risco ela também pode buscar por outras soluções mais econômicas e reavaliar novamente utilizando o nível de risco até que se consiga chegar em um patamar de eficácia.

Análise de Riscos na Segurança da Informação

Etapas da análise de risco



IMPORTANTE

É importante que a organização continue fazendo análises de riscos periodicamente, pois devido à volatilidade dos ambientes tecnológicos e do mercado acabam afetando o equilíbrio entre as vulnerabilidades e os recursos da organização.

O processo de análise de riscos está profundamente relacionado ao custo/benefício da implementação dos controles de segurança. Muitas empresas não conseguem por questões financeiras programar tais medidas, enquanto outras acham que são as medidas que não são necessárias no seu contexto econômico. Mas, vale ressaltar aqui a importância dos sistemas de segurança não só para as organizações, mas, também para seus clientes.

Políticas de Segurança

As informações, como vimos anteriormente, são ativos muito importantes para as organizações e com o passar dos anos tornou-se quase obrigatório o uso da tecnologia da informação para aperfeiçoar os processos de trabalho e não deixar que a empresa perca sua competitividade.

Os documentos que antes eram armazenados em armários começaram a ser transferidos para os computadores, deixando de ser um documento físico para ser um dado informático ou um ativo intangível. Devido a este processo de migração e a importância cada vez maior das informações é necessário que sejam aplicadas medidas de segurança a fim de preservar os dados da instituição de futuras ameaças.

Mas, antes de tudo deve-se definir um conjunto de regras a serem aplicadas por toda a organização com o propósito de estabelecer a padrões e procedimentos de segurança de forma clara e objetiva, estipulando uma conscientização geral aos usuários de definir as atribuições sobre o uso da informação e os riscos dos ataques. Deste modo, as empresas devem criar Políticas de Segurança da Informação (PSI).

A partir de agora, procuraremos responder algumas perguntas: E o que é uma PSI? Como funcionam? Quais são seus objetivos?. Vamos lá!

Políticas de Segurança

O que é uma Política de Segurança da Informação (PSI)?

Documento, desenvolvido pelas organizações, que **definem as políticas de segurança da informação na empresa**. São onde se estabelecem os princípios, compromissos, orientações e responsabilidades para que seja alcançado um padrão desejável de segurança. Além dos valores estabelecidos pela PSI, também são delineados os padrões e procedimentos de segurança com o objetivo de diminuir a probabilidade de ocorrência de incidentes.

As PSI são construídas levando em conta as características de cada empresa e a partir das necessidades enfrentadas pelo negócio, sendo implementada em uma abordagem *top-down* (de cima para baixo), partindo da diretoria da empresa para os demais funcionários.

Políticas de Segurança

O que é uma Política de Segurança da Informação (PSI)?

As PSI devem ser:

- **Aperfeiçoadas**, eventualmente, pela experiência do gestor e no decorrer do surgimento das necessidades. É importante se atentar para a revisão das políticas sempre que for identificado fatos novos e periodicamente, pois uma **política de segurança desatualizada pode abrir brechas para as ameaças**. Segundo a NBR ISSO/IEC 27002 (2013)

Convém que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

- **Comunicadas** aos funcionários para que seja entendida sua importância no âmbito da organização como um todo, podendo ser apresentadas em programas de capacitação dos funcionários. Sendo importante que os dirigentes da empresa apoiem e participem da implantação das políticas, a fim de dar relevância ao conteúdo explicitado.

Políticas de Segurança

Elaboração da Política de Segurança da Informação (PSI)

As PSI são guiadas pelos pilares da segurança da informação (confidencialidade, integridade e a disponibilidade) que são princípios básicos para alcançar a eficácia na segurança. A elaboração da PSI é dividida em quatro etapas distintas que se completam que são:



Políticas de Segurança

Elaboração da Política de Segurança da Informação (PSI)

Diagnóstico

Antes de começar a elaborar a política de segurança, deve-se fazer um levantamento das informações da empresa. Assim como foi feito na análise de riscos deve ser feito no diagnóstico das PSI.

Nesta etapa, deve-se conhecer os ativos de informação da sua empresa, assim como o nível crítico dos recursos, hierarquizando por importância na empresa e avaliando as ameaças e vulnerabilidades de cada um dos recursos.

Na fase do diagnóstico é interessante trabalhar junto com a análise de riscos, pois os dados da análise vão ao encontro do diagnóstico das PSI.

E por fim é imprescindível verificar se já existe alguma política de segurança da informação, às vezes, até feito por praxes de alguns funcionários de TI como controles de acesso os praticas de backups.

A função do diagnostico é analisar as informações existentes na organização, considerando:

- O nível critico das informações;
- A avaliação das vulnerabilidades e ameaças existentes;
- Verificar a existência de alguma política de segurança;
- Levantamento de todas as informações que devem ser protegidas.

Políticas de Segurança

Elaboração da Política de Segurança da Informação (PSI)

Planejamento

Usa por base as informações identificadas no diagnóstico, criando assim uma PSI que atenda as demandas da organização.

Esta fase irá determinar o planejamento estratégico, tático e operacional da PSI, auxiliando os gestores a pensar a organização a longo, médio e curto prazo, definindo suas estratégias, metas e seus objetivos para melhorar continuamente a segurança da empresa.

Além disso, dever-se ver o alinhamento das estratégias da empresa com a suas características intrínsecas como: o estágio de maturidade; grau de informatização; a sua área de atuação; e a cultura organizacional. Todas essas características devem ser levadas em conta para que se possa elaborar uma PSI com sucesso.

Políticas de Segurança

Elaboração da Política de Segurança da Informação (PSI)

Elaboração

Na fase de elaboração da PSI é necessário uma equipe preparada para que as atribuições das responsabilidades da segurança da informação estejam em conformidade com as políticas de segurança. Para isso, é necessário uma equipe que contenha profissionais de todos os setores da instituição, já que a segurança da informação não se delimita somente aos profissionais de TI e sim a toda a organização.

Nesta etapa, utilizando o planejamento e o diagnóstico feito, serão elaborados um conjunto de regras dividido em:

- **Políticas:** é considerado o texto que dá direcionamento geral, demonstrando os objetivos e intenções da empresa.
- **Padrões:** são exposições mais específicas delimitando os critérios necessários para estabelecer o controle dos recursos tecnológicos.
- **Procedimentos:** são apresentações descritivas, a fim de atingir os resultados esperados, como “passo a passo”.



Políticas de Segurança

Elaboração da Política de Segurança da Informação (PSI)

Elaboração

São vários tópicos que podem ser apresentados na elaboração de uma PSI, como por exemplo:

- Definição de metas, objetivos e princípios relativos à segurança da informação;
- Políticas de Backup;
- Procedimentos de controle de acesso;
- Criação de análises de riscos;
- Padrões mínimos de qualidade;
- Planos de treinamento em segurança da informação;
- Práticas de controle criptográfico.

As políticas devem ser escritas de forma clara para que não gere dúvidas.

Depois de pronto o PSI deve ser aprovado pelos líderes e gestores para somente assim ser liberado para prosseguir para a próxima etapa.



Políticas de Segurança

Elaboração da Política de Segurança da Informação (PSI)

Implementação

Chegamos a última etapa do processo de elaboração de uma PSI. Nesta fase, depois do documento aprovado pelos líderes e gestores ele está pronto para ser implementado.

Primeiramente, é essencial que se faça uma divulgação com todos os integrantes da organização, visando apresentar a PSI de forma geral. Por exemplo, fazendo uma palestra geral que mostre o porquê de se constituir uma PSI.

Após a palestra é preciso fazer treinamentos com a finalidade de mostrar de forma mais específica o conteúdo da PSI. Além disso, é importante disponibilizar avisos, guias de consultas e apoio especializado para tirar dúvidas.

Segundo a NBR ISSO/IEC 27002 (2013)

“Muitas organizações atribuem a um gestor de segurança da informação a responsabilidade global pelo desenvolvimento e implementação da segurança da informação, e para apoiar a identificação de controles. Entretanto, a responsabilidade por pesquisar e implementar os controles frequentemente permanecerá com os gestores individuais. Uma política comum é a nomeação de um proprietário para cada ativo que, então, se torna responsável por sua proteção no dia-a-dia”.

Políticas de Segurança

Elaboração da Política de Segurança da Informação (PSI)

Controle

O controle não é formalmente uma fase da elaboração da PSI, porém é um processo bastante valioso. Por conseguinte, esta etapa, é responsável por verificar como está a aplicação PSI. Transformando os problemas encontrados, em retorno para tentar melhorá-la.

Destaco ainda que é indispensável periodicamente revisar a PSI com os retornos fornecidos pelo controle para mantê-la sempre atualizada.



IMPORTANTE

Caso queira conhecer melhor as práticas de elaboração de políticas de segurança existe a norma ISSO/IEC 27002 (2013), fornecida pela ABNT (Associação Brasileira de Normas Técnicas)



Nossa jornada termina aqui, porém devo lembrar que leiam os materiais complementares que foram expostos nos temas como vídeos, artigos e documentos.

Façam as questões avaliativas e as atividades dispostas no curso, para que possa assimilar melhor o conteúdo de forma prática e não se esqueçam de aplicar os conteúdos aprendidos no seu cotidiano pessoal ou na área de trabalho.

Leiam quantas vezes for necessário o material para que possam assimilar os conceitos.

O que você estudou

Tema 1 – Introdução ao assunto Segurança da Informação

- Conceituamos informação e aprendemos sobre sua importância.
- Definimos o conceito de Tecnologia da Informação, destacando seus parâmetros econômicos e sociais.
- Entendemos o sistema de informação, utilizando conceitos básicos como dado, informação e conhecimento, que subsidiam sua melhor compreensão.
- Conceituamos segurança da informação, destacando seus aspectos históricos e entendendo sobre crimes virtuais.

O que você estudou

Tema 2 – Princípios e conceitos da Segurança da Informação

- Estudamos os princípios da segurança da informação e seus pilares (confiabilidade, disponibilidade e integridade).
- Aprendemos sobre diferentes conceitos como: vulnerabilidade, ataque e atacantes, entre outros.

O que você estudou

Tema 3 – Gestão de processos de segurança

- Vimos que o Risco está associado à exploração de uma ou mais vulnerabilidades do sistema.
- Conhecemos os quatro fatores que envolvem a análise de risco (análise de ambiente, identificação, determinação e classificação).
- Aprendemos que a Política de Segurança da Informação (PSI) é um documento, desenvolvido pelas organizações, que definem as políticas de segurança da informação na empresa.
- Estudamos que a elaboração de uma PSI envolve: diagnóstico, planejamento, elaboração e implementação.



Glossário

TI – Tecnologia da Informação

SSD- Cartão de Memória

PSI – Política de Segurança da Informação

CD- Disco Compacto

Pen-Drive – Dispositivo de memória

ISO/IEC - Norma internacional de segurança da informação

ISTR - Relatório de ameaças à segurança na internet de 2017



Referências

- ABNT NBR ISO/IEC 27002:2013
 - ALBERTIN, A. L. Administração de informática: funções e fatores críticos de sucesso. 4 ed. São Paulo: Atlas, 2002. 178p.
 - CARDOSO, André lima; ARAUJO, Ricardo. ESTRATEGIA DIGITAL: VANTAGENS COMPETITIVAS na INTERNET. 2003. Editora: Ciência Moderna.
 - Claudia Dias, Segurança e Auditoria da Tecnologia da Informação, 2000, Editora: Axcel Books 142.
 - COCO, I. A. Desempenho do negócio é o valor de TI. Information Week Brasil, São Paulo, ano 10, n. 205, p. 49, jul. 2008.
 - DOS SANTOS, André Alencar. Informática Descomplicada. -6.ed. Brasília, v.1, 2012, Editora: Vestcon.
 - FOINA, Paulo Rogério. Tecnologia de informação: planejamento e gestão / Paulo Rogério Foina.
 - Hackers. TMRC. Disponível em: < <http://tmrc.mit.edu/hackers-ref.html> >.
 - KENN, Peter G. W. Guia Gerencial para a tecnologia da informação: Conceitos essenciais e terminologia para empresas e gerentes. Rio de Janeiro.
 - NORTON SYMANTEC, Relatório de ameaças à segurança na Internet, 2017.
 - NORTON SYMANTEC, Relatório de informações de segurança cibernética, 2016.
 - Robert N. Charette. Information Technology Risk Engineering.
 - ULBRICH, Henrique Cesar; VALLE, James Della. Digerati Books, ed. Universidade Hacker. 2006 5. ed. ed. São Paulo.
-
- Parte das imagens utilizadas neste trabalho foram retiradas do Pixabay e possuem a licença Creative Commons CC0.