Curso Técnico em Desenvolvimento de Sistemas Online

SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

GEEaD - Grupo de Estudo de Educação a Distância

Centro de Educação Tecnológica Paula Souza

Expediente

GEEaD – CETEC
GOVERNO DO ESTADO DE SÃO PAULO
EIXO TECNOLÓGICO DE INFORMAÇÃO E COMUNICAÇÃO
CURSO TÉCNICO EM DESENVOLVIMENTO DE SISTEMAS
FUNDAMENTOS DE INFORMÁTICA

Autores:
Marcelo Fernando Iguchi
Eliana Cristina Nogueira Barion

Revisão Técnica:
Lilian Aparecida Bertini

Revisão Gramatical:
Juçara Maria Montenegro Simonsen Santos

Editoração e Diagramação:
Flávio Biazim

São Paulo – SP, 2019

APRESENTAÇÃO

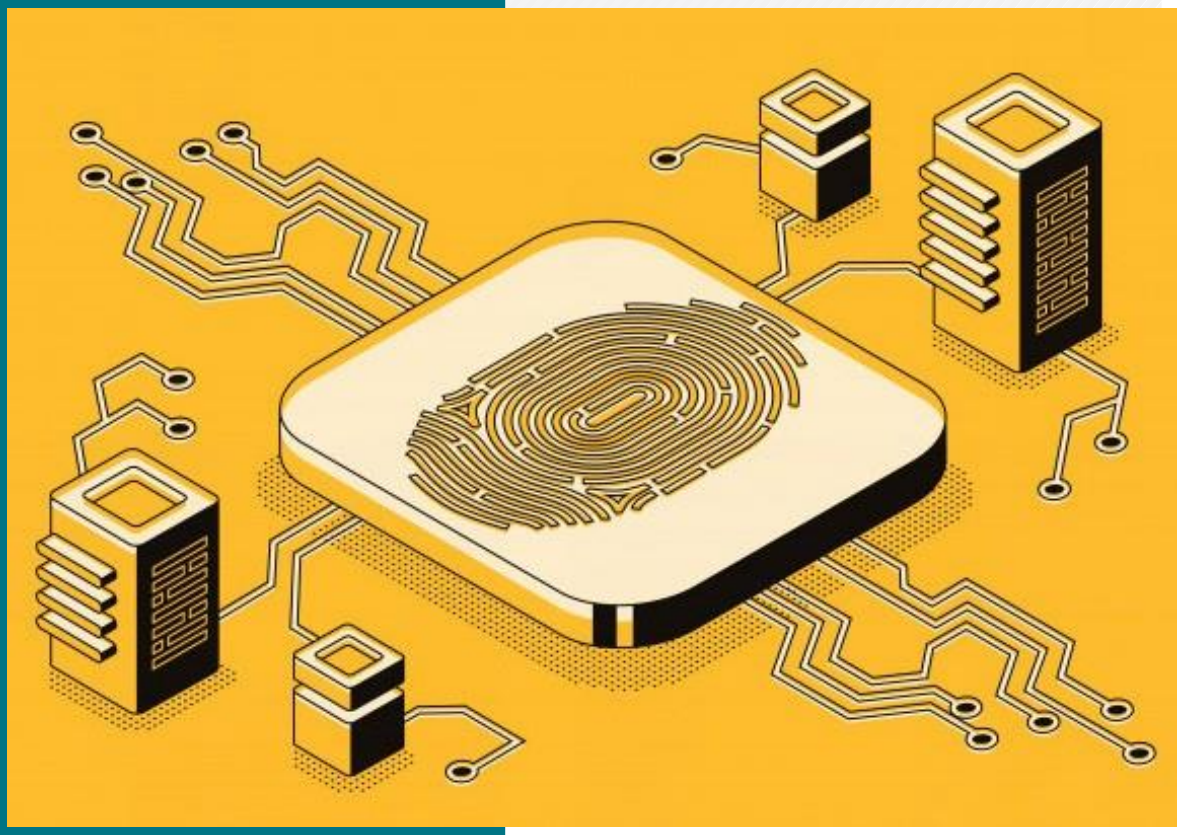
Este material didático do Curso Técnico em Desenvolvimento de Sistemas modalidade EaD foi elaborado especialmente por professores do Centro Paula Souza para as Escolas Técnicas Estaduais – ETECs.

O material foi elaborado para servir de apoio aos estudos dos discentes para que estes atinjam as competências e as habilidades profissionais necessárias para a sua plena formação como Técnicos em Desenvolvimento de Sistemas.

Esperamos que este livro possa contribuir para uma melhor formação e apefeiçoamento dos futuros Técnicos.

AGENDA 05

CONCEITOS DE SEGURANÇA DA INFORMAÇÃO



MERGULHANDO NO TEMA...

"O único sistema verdadeiramente seguro é aquele que está desligado, preso a um bloco de concreto, trancado em uma sala revestida de chumbo com guardas armados."

Eugene H. Spafford - Professor na Purdue University.

Diariamente nos expomos aos mais diversos riscos quando utilizamos os aplicativos de comunicação do telefone celular ou nossos computadores. De vez em quando escutamos notícias sobre problemas de segurança em um app X ou Sistema Operacional Y, porém só nos preocupamos realmente com a segurança das nossas informações digitais quando alguma fatalidade acontece. Como, por exemplo, quando ocorre um roubo do nosso telefone celular ou computador porque temos dados pessoais guardados neles.

O conceito de segurança da informação é bastante amplo e complexo. A segurança da informação possui vários níveis e tipos distintos desde a proteção de um dado ou senha pessoal, passando pela segurança corporativa até questões envolvendo a segurança nacional de um país.

Podemos definir Segurança da Informação como a preservação tríade Confidencialidade, Integridade e Disponibilidade das informações. Abreviando, teremos a sigla CID em português ou em inglês CIA (Confidentiality, Integrityand, Availability)

A **confidencialidade** consiste na privacidade dos dados. É a garantia que somente as pessoas que tenham autorização ou privilégios necessários possam acessar as informações que estão armazenadas ou em processamento em um sistema ou que são transmitidas por meio das redes de comunicação.

A **integridade** corresponde à consistência, precisão e confiabilidade das informações. Refere-se ao grau de confiabilidade da informação garantindo que não foram manipuladas sem as devidas permissões.

A **disponibilidade** garante que as informações estejam acessíveis as pessoas autorizadas sempre que forem necessárias garantindo a prestação do serviço sem interrupções.

Imagem 03

Mas que tipo de informação devemos proteger?

Basicamente devemos proteger todas as informações pessoais ou de uma organização que estão armazenadas em sistemas computacionais (servidores, discos, pen drives) ou impressas (papéis, microfilmes), que são transmitidas por meios de comunicação (e-mail, fax, comunicação de dados).
Resumindo protegemos todas as informações que podem causar danos, seja para uma única pessoa (dados pessoais) quanto para uma corporação. Você não passaria o número da sua conta bancária e senha para um desconhecido, passaria?

Por que devemos proteger as informações?

Devemos proteger as informações de sistemas digitais para nos prevenirmos dos mais variados golpes e fraudes presentes na internet, se pensarmos como pessoas físicas. Pensando como uma pessoa jurídica ou empresa protegemos as informações de espionagem industrial, hackers, gravações de comunicação, acessos não permitidos, empregados que agem de má fé, entre outros.
Contudo, antes de prosseguirmos devemos saber alguns conceitos, ou terminologias utilizadas na área:

- Vulnerabilidade: é uma fraqueza de um ativo ou sistema que podem ser exploradas para fins espúrios.

Pode ser física (hardware), lógica (software) ou envolvendo algum processo falho que comprometa o sistema.
Exemplo: um datacenter localizado em uma área potencialmente sujeita a desastres naturais, senhas fracas, falta de criptografia nos dados ou controle de acesso físico etc.

- Ameaça: modo como uma vulnerabilidade pode ser descoberta, causando um incidente de segurança.

Exemplo: falha de hardware, roubo.

- Risco: Probabilidade de comprometimento da segurança por parte de uma ameaça aproveitando-se de uma vulnerabilidade em um ativo.
- Proteção: Procedimento utilizado para diminuição de um risco.

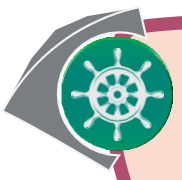
Exemplo: antivírus, firewall.

- Incidente: quando um ou mais propriedades da tríade CIA foram violados.

Mecanismos de Segurança

Segurança física

Sempre que pensamos em segurança da informação a primeira coisa que nos vem à mente são problemas com softwares de computador ou telefones móveis.
Muitas pessoas esquecem do mais essencial antes de protegermos os programas. Devemos proteger o equipamento físico ou hardware. Sem essa proteção de nada adiantará protegermos a parte lógica.
O objetivo de protegermos fisicamente o equipamento e as informações contidas neles é impedir o acesso não autorizado aos recursos de hardware.



VOCÊ NO COMANDO

Você saberia dizer quais tipos de controles de acesso físico poderiam ser utilizados?

Veja se você acertou...

Os controles de acesso podem e devem incluir identificação pessoal por meio de catracas, utilização de crachás, biometria, sala-cofre para a entrada em área restrita.

Devemos ter em mente que a área onde fica a infraestrutura da sala de comunicação e armazenamento de dados de uma empresa deva ser uma área com acesso físico restrito com controle estrito de entrada e saída de equipamentos, inclusive dispositivos móveis como notebooks, celulares e pen-drives. Podem ser agregados também controle de intrusão e monitoramento por CFTV (Circuito Fechado de Televisão).

Imagem 04

Deve-se pensar também que catástrofes podem acontecer, portanto, é preciso avaliar e tomar precauções quanto ao risco de inundações, incêndios, problemas elétricos, climatização.

Segurança Lógica

A segurança lógica inclui tudo que está relacionado ao sistema lógico como os dados que estão contidos no hardware e são acessados por pessoas ou outros sistemas.

O controle de acesso deve ser feito por meio da utilização de senhas, listas de controle de acesso, criptografia, firewall. As ações realizadas no sistema devem ser monitoradas por meio da utilização de arquivos de registros de atividades (logs).

O ideal para um maior nível de segurança é que seja feita uma convergência entre segurança física e lógica, criando dessa forma uma série de procedimentos institucionalizados que devem ser divulgados para todos os colaboradores da empresa. Isso porque apesar de tomar todas as precauções físicas e lógicas quem garante a segurança do sistema implementado, são as pessoas, portanto, que devem ser o alvo da conscientização.

Para conhecer um pouco mais sobre segurança física e lógica, acesse a publicação "Mantenha a segurança física e lógica da informação".
Link: https://www.portaleducacao.com.br/conteudo/artigos/administracao/mantenha-a-seguranca-fisica-e-logica-da-informacao/55243 - acessado em 06/09/2018.

Políticas de Segurança

Política de Segurança (PS) da Informação são um conjunto de procedimentos e regras que gerenciam as informações e equipamentos de uma empresa. Elas devem ser seguidas por todos os funcionários, colaboradores sejam eles internos ou externos como prestadores de serviços.

O objetivo da PS é proteger a confidencialidade a integridade e disponibilidade das informações empresariais evitando riscos desnecessários provenientes da má utilização dos equipamentos. Com a redução dos riscos tenta-se também minimizar os eventuais danos provocados por algum incidente que ocorra. Para tanto o ambiente do sistema de informação deve ser monitorado constantemente para verificar se está sendo

utilizado corretamente e, também para procurar falhas e correções o mais breve possível. Mesmo que isso inclua uma alteração nas políticas de segurança.

A PS deve ser coordenada e implementada, preferencialmente, por especialistas da área de segurança de informação em conjunto com os administradores da empresa. É importante salientar que PS não deve ficar restrita somente a área de Tecnologia da Informação, mas deve abranger a empresa como um todo. Ela deve se integrar à visão, à missão, as metas e os valores do negócio como um todo.

Para elaborarmos uma boa política de segurança devemos nos atentar aos seguintes itens:

- Definição dos processos ou recursos prioritários para definir as prioridades de segurança;
- Classificação das informações como confidenciais ou públicas;
- Definição dos objetivos de segurança da informação da instituição;
- Realização de análise de risco;
- Padronização de qualidade que os sistemas devem atender;
- Controle de acesso aos recursos e sistemas computacionais
- Uso da rede, incluindo intranet e internet;
- Normatização dos procedimentos dos usuários;
- Definição dos direitos e deveres dos usuários;
- Instalação de programas de computador;
- Utilização de e-mails, sejam eles corporativos ou pessoais;
- Regras para criação e utilização de senhas de acesso;
- Regras para utilização de equipamentos pessoais tais como notebooks, telefones celulares, pen-drives, mídias externas, entre outros na rede interna;
- Utilização de antivírus;
- Métodos de supervisão das violações da PS estabelecida;
- Estabelecimento claro das punições relativas a violação da PS vigente;
- Auditoria;
- Backup das informações;
- Princípio da continuidade de negócio em casos adversos;

Uma vez elaborada a PS é preciso garantir que esta seja amplamente divulgada e que todos os colaboradores internos e externos da instituição tenham amplo acesso a ela, bem como o treinamento adequado no que tange aos seus direitos, deveres e procedimentos a serem seguidos cotidianamente, a fim de se evitar futuros questionamentos legais, principalmente quando algum dos itens constantes forem violados.

E finalmente, uma vez criada, definida e divulgada a política de segurança, essa não deve ser esquecida, mas deve ser constantemente atualizada, conforme as necessidades da organização.

Backup

O Backup é uma cópia de segurança dos dados de um dispositivo em algum outro como um HD externo, em outro computador ou servidor ou atualmente na famosa nuvem (internet).

Em geral, os usuários não dão muito valor ao backup até que algum desastre ocorre como um HD corrompido, um pen drive perdido ou mesmo uma fatalidade maior como o roubo de um laptop ou telefone celular.

Imagem 05

Para um usuário doméstico perder algumas fotos, vídeos ou música traz algum transtorno ou perda emocional, caso sejam conteúdos que registrem momentos de nossas vidas como festas, casamentos, viagens ou filhos, mas, muitas vezes não trazem prejuízos financeiros.

Agora, imagine para uma empresa onde um servidor de comércio eletrônico tenha um HD inutilizado por um raio proveniente de uma tempestade com dados de clientes, fornecedores, estoque e transações realizadas.

É um transtorno financeiro de milhares ou até centenas de milhares de reais que pode fazer uma empresa fechar as portas.

Por esse motivo, as empresas devem ter sempre um ou mais de um backup para garantir a continuidade de seus negócios em caso de um desastre, evitando dessa forma a perda de informações.

Outra recomendação é que a cópia de segurança não seja feita nunca na mesma máquina onde se situam os dados originais. Se possível, ela deve ser feita em outro local (outra mídia removível como um HD externo, outro servidor ou outro data center) com uma boa distância física para salvaguardar as informações. Isso tem sido lição aprendida a duras penas para muitas empresas de TI.

Com o atentado de 11 de setembro, muitas empresas pensavam que tendo um backup no outro prédio das torres gêmeas era o suficiente. Mas não foi. As duas construções foram ao chão e muitas dessas empresas não se recuperaram.

Para conhecer os tipos de backup existentes, vamos assistir ao vídeo “Backup e seus tipos”. Uma Videoaula do Dicionário de Informática. Disponível em https://www.youtube.com/watch?v=NIqInobRLIs. Acessado em 06/09/2018.

Firewall ou traduzindo livremente para o português: parede de fogo. Um firewall pode ser um hardware, um software ou uma combinação de ambos e nada mais é do que um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída, decidindo se permite ou bloqueia a passagem dos dados de acordo com as regras definidas para o seu funcionamento.

Criptografia e Firewall

Imagem 06 - Firewall por Hardware

O firewall é o responsável por analisar o tráfego da rede bloqueando a entrada de possíveis conteúdos maliciosos. Resumindo, eles protegem as redes internas colocando uma barreira antes de atingir a rede externa como a internet.
Os usuários domésticos estão habituados a utilizar soluções do tipo Internet Security que englobam um anti-vírus e um firewall e está de bom tamanho para a proteção doméstica.
Mas para as empresas é necessário um controle mais estrito do tráfego das informações e por isso muitas vezes elas utilizam uma combinação de um firewall por hardware e software. O firewall por hardware é um equipamento físico projetado especificamente para isso podendo atuar com softwares instalados na rede ou nos computadores locais individuais.

Curiosidade: saiba que o próprio Windows possui um firewall embutido e ativado por padrão chamado Windows Defender Firewall.

A palavra criptografia vem da junção das palavras gregas kryptós que significa oculto com Gráphein que quer dizer escrita. Logo, trata-se de uma técnica onde uma mensagem original é codificada utilizando um artifício, ou atualmente um algoritmo matemático, para que, se caso ela seja interceptada não seja possível a sua leitura sem a sua decodificação.
Foi muito utilizada em períodos de guerra para comunicações militares e hoje, além disso, é usada também para manter o sigilo no armazenamento de dados sensíveis e nas telecomunicações para o envio de senhas, transações bancárias, mensagens instantâneas etc.

Para conhecer mais sobre a criptografia em TI, acesse o vídeo "O que é criptografia", disponível em https://www.youtube.com/watch?v=zkq-fiXGSkM. Acessado em 06/09/2018.

Um exemplo de criptografia rudimentar é quando crianças, como forma de brincadeira, escrevem uma mensagem com suco de limão que ao secar no papel fica invisível. E somente ao aquecermos um pouco o papel com uma chama de uma vela, por exemplo, a mensagem é revelada.
É importante uma empresa armazenar, transportar ou transferir os seus dados sigilosos de modo criptografado, pois se ocorrer algum problema como perda de dispositivos ou ataques hackers essas informações não sejam comprometidas.

EXERCITANDO APRIMORANDO

1. Defina os conceitos de Confidencialidade, Integridade e Disponibilidade.
2. Qual é a importância do Backup para uma organização.
3. O que é criptografia.
4. É importante uma instituição possuir uma política de segurança. Por que?
5. Cite exemplos de segurança física de uma instalação de TI.

Respostas:

1. Confidencialidade é quando garantimos que a informação só pode ser acessada por pessoas autorizadas. Integridade é a proteção da exatidão da informação e Disponibilidade é a garantia de que a informação pode ser acessada sempre que requisitada pelas pessoas autorizadas.

2. Para uma empresa manter uma rotina ou política de backup é fundamental pois caso ocorra uma eventualidade com os dados originais o funcionamento não seja interrompido (continuidade de negócios).

3. A criptografia é uma técnica utilizada para se codificar uma mensagem ou dados a fim de que estes não sejam entendidos caso sejam interceptados por terceiros.

4. Para uma empresa ser segura no âmbito digital é importante ter uma política de segurança robusta, pois é ele que definirá quais são as normas e procedimentos que serão utilizados com os recursos de TI da empresa garantindo a tríade da CIA. Ela estabelece também o que deve ser feito em casos de inconformidades no sistema, estabelecendo inclusive punições aos infratores.

5. Alguns exemplos que podemos citar de segurança física de um ambiente de TI são controle de acesso utilizando crachás, senhas de acesso ou biometria, sala-cofre, circuito fechado de monitoramento por câmeras de segurança (CFTV).