EDUCAR PARA TRANSFORMAR

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Prof(a): Odecília Barreira

odecilia.benigno@estacio.br

TEMA DA AULA

EDUCAR PARA TRANSFORMAR

PRINCÍPIOS DA SEGURANÇA E O CICLO DE VIDA DA INFORMAÇÃO

OBJETIVOS:

- SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO.

Situação-problema:

EDUCAR PARA TRANSFORMAR

Falhas de segurança e vazamento de dados são noticiados frequentes no mundo inteiro.

- Com base no artigo publicado no Jornal ´Diário do Nordeste em 2018: O Banco Inter teria sido objeto de uma extorsão, tomando como base informações de seus clientes. Os autores da ameaça exigiam pagamento para não colocar informações de 100 mil correntistas na internet. No mesmo dia, em nota, o banco prestou esclarecimentos. 'O Banco Inter foi vítima de tentativa de extorsão e imediatamente constatou que não houve comprometimento da segurança no ambiente externo e nem danos à sua estrutura tecnológica'.

- Artigo disponível em: (https://diariodonordeste.verdesmares.com.br/pais/ministerio-publicoabre-inquerito-para-apurar-vazamento-de-dados-do-banco-inter-1.1937804).

Situação-problema:

EDUCAR PARA TRANSFORMAR

- E então, você utiliza serviços da Vivo, Whatsapp, Facebook? Eles também foram vítimas de ataques cibernéticos.

- Que tipos de controles as empresas devem adotar para minimizar as chances da concretização do ataque e a dimensão do impacto?

- O avanço tecnológico estimula as empresas independente do seu porte a acompanhar essa evolução a fim de se adequar e garantir seu crescimento no mundo virtual e físico.
- Assim, profissionais de T.I e de Segurança da Informação são desafiados continuamente a identificar riscos e implementar controles a fim de minimizar a exploração de vulnerabilidade e consequentemente os impactos causados.

- Segundo a norma NBR ISO/IEC 27002:2005:
  - A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.
  - Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

TIPOS DE CONTROLE

EDUCAR PARA TRANSFORMAR

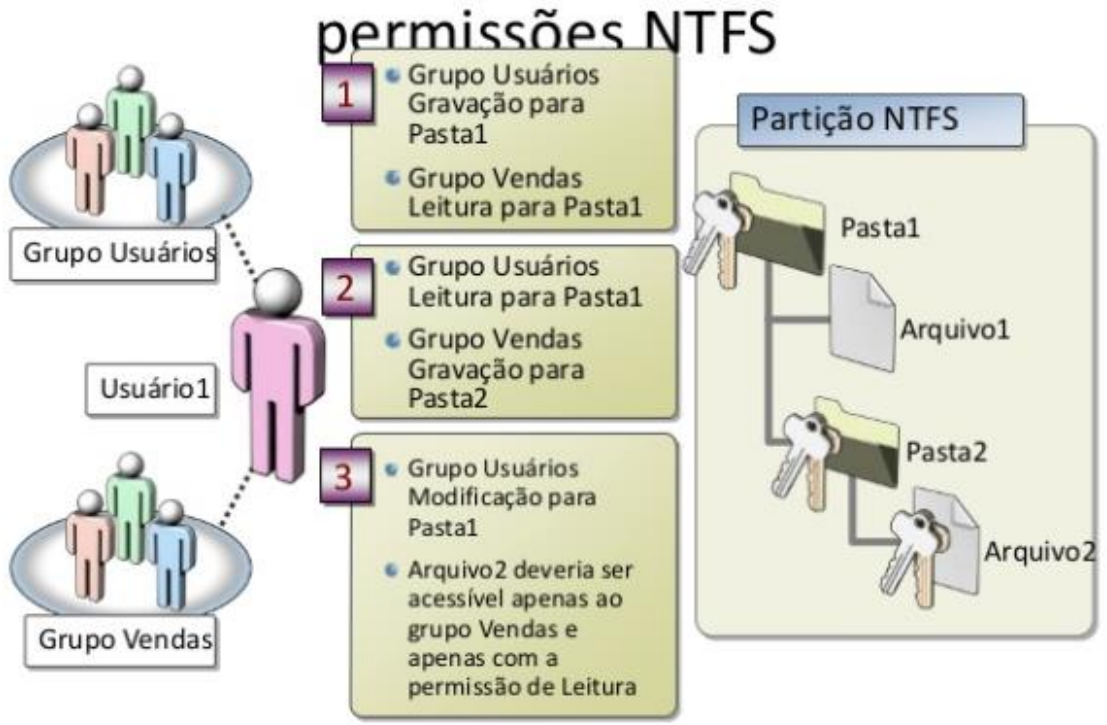
- Lógicos (senhas, sistemas de biometria etc);
- Físicos (leitores biométricos, câmeras, catracas, portas corta-fogo, etc);
- Administrativos (Políticas de segurança).

- Mas, como saber quais controles devem ser adotados?
  - É necessários avaliar riscos em relação aos ativos organizacionais.

Controles de Acesso

EDUCAR PARA TRANSFORMAR

Controle de Acesso



Sistemas de Controle de Acesso

EDUCAR PARA TRANSFORMAR

Quem tem as chaves da sua casa?

As regras para controlar acesso a informação deve ser adotada pelas empresas via políticas de segurança.

Mesmo que o usuário seja identificado e autenticado, ele deve visualizar somente as informações permitidas e de acordo com seu nível de hierarquia e responsabilidade dentro da empresa.

Para isso é necessário restringir o acesso em relação a aplicações, arquivos e utilitários que o usuário pode ter acesso.

O controle de acesso evita que as pessoas não autorizadas visualizem e editem dados que causem comprometimento a organização além de prevenir o roubo de informações confidenciais.

Controle de Acesso

- O controle de acesso deve ser desenvolvido com base nos requisitos de negócio e segurança da organização.
- Premissa: Tudo é proibido exceto o que é expressamente permitido.

Quadro 2.1 Relação de privilégios e produto.

Cargo	Consultar produto	Alterar produto	Incluir produto	Excluir produto
Vendedor	Permitido			
Vendedor sênior	Permitido	Permitido		
Gerente	Permitido	Permitido	Permitido	Permitido

Política de Segurança

EDUCAR PARA TRANSFORMAR

- A política de segurança é elaborar um documento que deverá conter as regras e procedimentos que os colaboradores e empresa deverão adotar, tais como:
  - Senhas;
  - Backup;
  - Privacidade;
  - Confidencialidade.

  - Após a definição do documento de políticas de segurança, elas deverão ser divulgadas para todos os funcionários da empresa e a partir de então devem ser praticadas.

Sistemas de Identificação e Autenticação de Usuários

EDUCAR PARA TRANSFORMAR

- Com o surgimento e aumento das redes abertas como wi-fi, aumentou também o número de diversos crimes digitais, entre eles roubo de senhas e interceptação de dados confidenciais.
- Daí a importância de utilizar meios de identificar e autenticar seus usuários, para tentar garantir a segurança de suas informações.

Sistemas de Identificação e Autenticação de Usuários

EDUCAR PARA TRANSFORMAR

Há três categorias de autenticação de usuários:

1. Autenticação por conhecimento: O que se sabe. Utiliza informações que somente o usuário saiba, tais como: senhas e perguntas pessoais.
2. Autenticação por propriedade: O que se possui. Utiliza informações fornecidas por objetos físicos, como cartões magnéticos, chips, smart cards ou tokens.
3. Autenticação por características: O que se é. Utiliza informações do usuário que o diferencia dos demais, por meio de um aspecto físico ou comportamental, como a prova por biometria.

Sistemas de Identificação e Autenticação de Usuários

EDUCAR PARA TRANSFORMAR

- Senhas descartáveis
  - As senhas descartáveis são geradas automaticamente e tem validade de apenas alguns segundos. Assim que a senha expira, outra é gerada, o que dificulta o seu roubo e utilização.
  - Exemplo: Senhas geradas por tokens de bancos

Sistemas de Identificação e Autenticação de Usuários

EDUCAR PARA TRANSFORMAR

- **Biometria** é a ciência que estuda as características comportamentais e físicas do ser humano por meios de medições biológicas.
- Exemplos de características comportamentais:
  - Reconhecimento de assinaturas em cheques método bastante utilizado pelos bancos, porém a forma de escrita pode se alterar com o decorrer dos anos e em situações de estresse.
  - Esse tipo de autenticação está cada vez mais sendo substituídas pelas características físicas.
- Exemplos de características físicas:
  - Impressão digital, íris (olhos), retina (olhos), voz, rosto, geometria da mão.

Proteção Perimetral

Para definir uma proteção perimetral é importante que sejam definidas quais os pacotes de dados podem trafegar livremente na organização e quais deverão ser barrados.

Alguns exemplos de mecanismos de proteção.

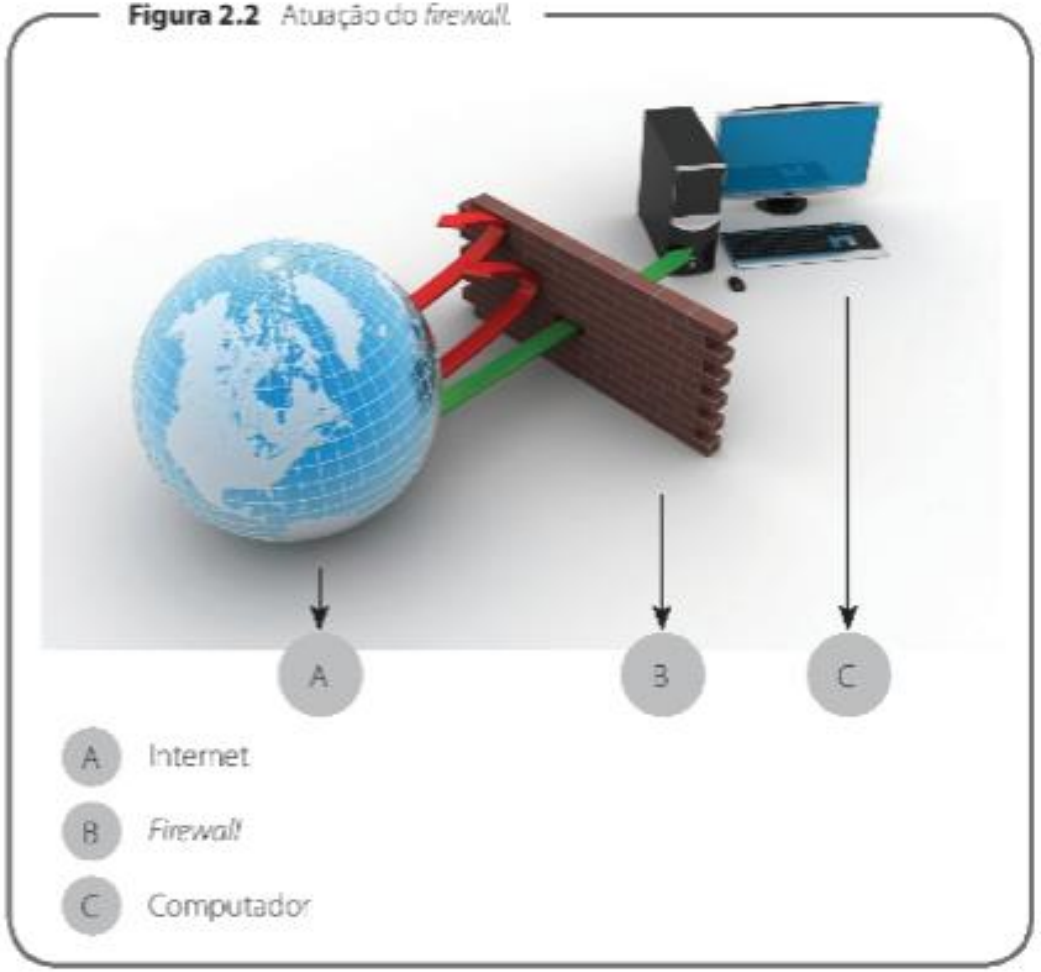
- Agentes proxy
- Firewall
- Antivírus
- Intrusion Detection systems (IDS)

O mecanismo de proteção mais utilizado atualmente é o firewall.

Um firewall é um software ou um hardware que confere informações originadas de uma rede ou da internet.

Sua função é bloquear ou permitir que essas informações acessem um computador ou uma rede, dependendo da configuração realizada no firewall.

Figura 2.2 Atuação do *firewall*.



Quarta → continuar desse ponto.

Regras de Firewall

EDUCAR PARA TRANSFORMAR

[blk_BL_socialnet]	access	deny
[blk_BL_spyware]	access	deny
[blk_BL_tracker]	access	----
[blk_BL_updatesites]	access	----
[blk_BL_urlshortener]	access	----
[blk_BL_violence]	access	----
[blk_BL_warez]	access	----
[blk_BL_weapons]	access	----
[blk_BL_webmail]	access	----
[blk_BL_webphone]	access	----
[blk_BL_webradio]	access	----
[blk_BL_webtv]	access	----
Default access [all]	access	allow

Target Rules List (click here)

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories

[blk_BL_adv]	access	----
[blk_BL_aggressive]	access	deny
[blk_BL_alcohol]	access	----
[blk_BL_anonvpn]	access	----
[blk_BL_automobile_bikes]	access	----
[blk_BL_automobile_boats]	access	----
[blk_BL_automobile_cars]	access	----
[blk_BL_automobile_planes]	access	----
[blk_BL_chat]	access	----
[blk_BL_costtraps]	access	----
[blk_BL_dating]	access	----
[blk_BL_downloads]	access	----
[blk_BL_drugs]	access	deny
[blk_BL_dynamic]	access	----
[blk_BL_education_schools]	access	----
[blk_BL_finance_banking]	access	----
[blk_BL_finance_insurance]	access	----
[blk_BL_finance_moneylending]	access	----
[blk_BL_finance_other]	access	----
[blk_BL_finance_realestate]	access	----
[blk_BL_finance_trading]	access	----
[blk_BL_fortunetelling]	access	----
[blk_BL_forum]	access	----
[blk_BL_gamble]	access	----
[blk_BL_government]	access	whitelist

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

- Os termos: riscos e ameaças organizacionais são situações externas, pertencentes ao tempo atual ou futuras, que, se não eliminadas, minimizadas ou evitadas pela empresa, podem (ou poderão) afetá-la negativamente.
- No Livro “A Arte da Guerra”, o autor Zun Tsu coloca:
  - “Se conhecemos o inimigo (ambiente externo) e a nós mesmos (ambiente interno), não precisamos temer o resultado de uma centena de combates.
  - Se nos conhecemos, mas não ao inimigo, para cada vitória sofreremos uma derrota.
  - Se não nos conhecemos nem ao inimigo, sucumbiremos em todas as batalhas.”

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

O risco é inevitável. Por exemplo, quando:

- Investidores compram ações;
- Cirurgiões realizam operações;
- Engenheiros projetam pontes;
- Empresários abrem seus negócios, etc.

Ou seja, administrar os riscos – que sempre irão existir – torna-se estratégico e, além disto, pode vir a se transformar em oportunidades. Portanto, deve-se transcender o "medo aos riscos" para "saber lidar de forma estratégica com os riscos".

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

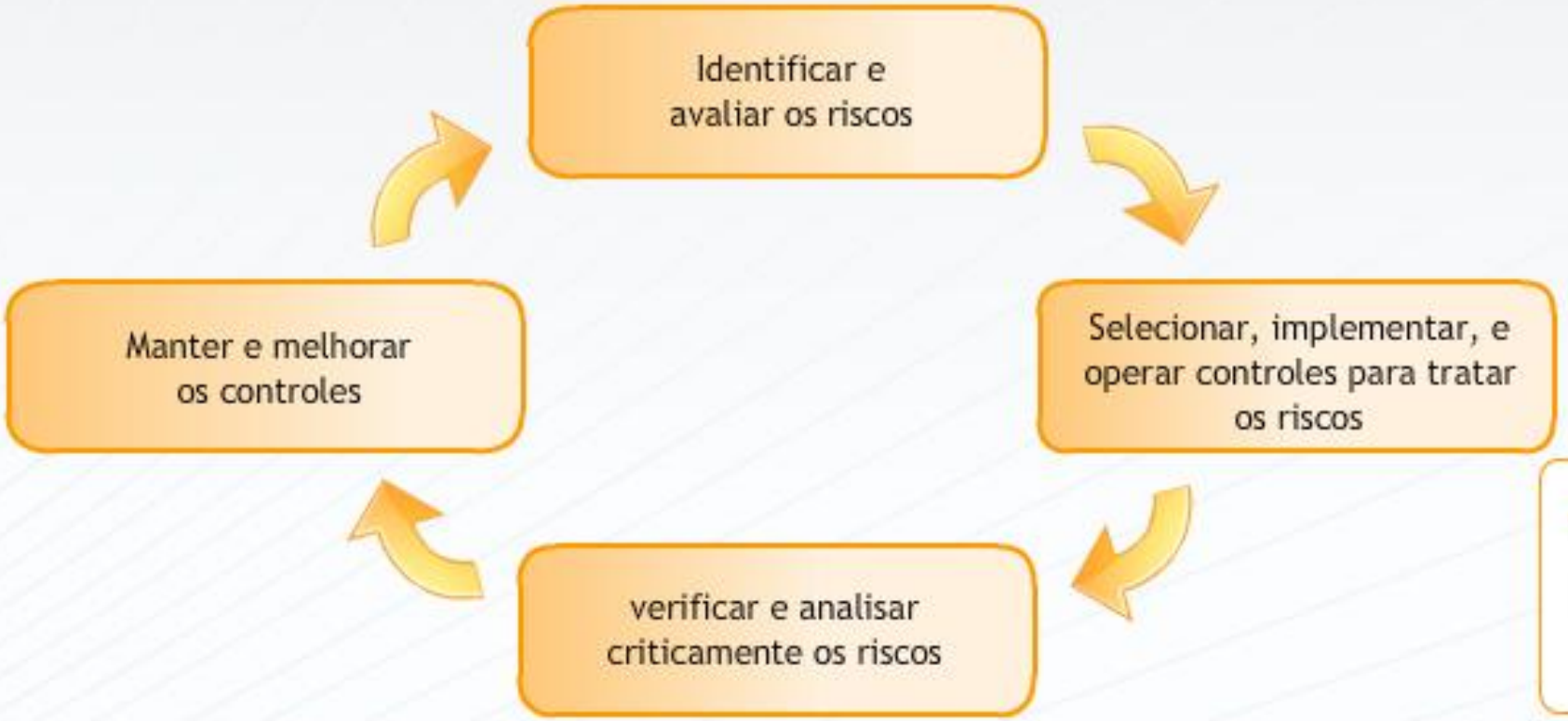
- Na área de tecnologia da informação e comunicação:
  - Risco é considerado como o impacto negativo, motivado pela exploração de uma vulnerabilidade, considerando a possibilidade e o impacto da sua ocorrência.
- O processo para identificar, mensurar e planejar passos para reduzir um determinado risco a níveis aceitáveis pela organização é definido como Gerenciamento de Riscos (STONEBURNER, 2002 apud GONÇALVES, 2008, p. 15)

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Etapas da Gestão de Risco

A gestão de riscos contempla uma série de atividades relacionadas à forma como uma organização lida com o risco e utiliza o ciclo do PDCA, que nos permite entender a gestão do Risco como um processo contínuo:



SAIBA MAIS

Clique aqui e saiba mais sobre as Etapas da Gestão de Risco.

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Tratamento dos riscos

Fase em que selecionamos e implementamos medidas de forma a reduzir os riscos que foram previamente identificados. Existem várias classificações disponíveis para as medidas de proteção. Segundo Beal, uma classificação possível é:

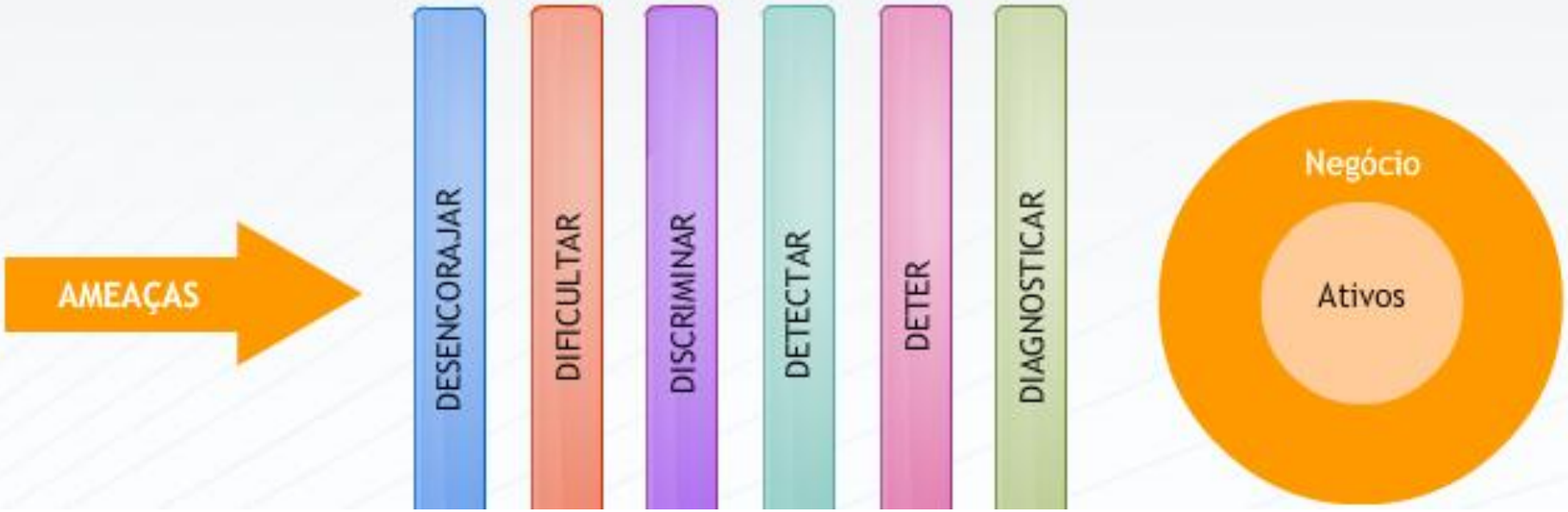
Medidas preventivas	Controles que reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente/ativo;sistema, reduzindo assim a probabilidade de um ataque e/ou sua capacidade de gerar efeitos adversos na organização.
Medidas corretivas ou reativas	Reduzem o impacto de um ataque/incidente. São medidas tomadas durante ou após a ocorrência do evento.
Métodos detectivos	Expõem ataques/incidentes e disparam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita.

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Riscos, medidas de segurança e o ciclo de segurança

Segundo Sêmola, para um melhor entendimento da amplitude e complexidade da segurança, é comum estudarmos os desafios em camadas ou fases para tornar mais claro o entendimento de cada uma delas. Estas fases são chamadas de **barreiras** e foram divididas em seis. Cada uma delas tem uma participação importante no objetivo maior de reduzir os riscos, e por isso, deve ser dimensionada adequadamente para proporcionar a mais perfeita integração e interação:



Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Barreira1: Desencorajar

Esta é a primeira das cinco barreiras de segurança e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou podem perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou humanos. A simples presença de uma câmara de vídeo, mesmo falsa, de um aviso de existência de alarmes, já são efetivos nesta fase.

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Riscos, medidas de segurança e o ciclo de segurança.

Barreira 02: Dificultar

O papel desta barreira é complementar à anterior através da adoção efetiva dos controles que irão dificultar o acesso indevido. Podemos citar os dispositivos de autenticação para acesso físico, por exemplo.

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Riscos, medidas de segurança e o ciclo de segurança.

Barreira 03: Discriminar

Aqui o importante é se cercar de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e banco de dados.

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Riscos, medidas de segurança e o ciclo de segurança.

Barreira 04: Detectar

Esta barreira deve munir a solução de segurança de dispositivos que sinalizem , alertem e instrumentem os gestores da segurança na detecção de situações de risco. Seja uma tentativa de invasão ou por uma possível contaminação por vírus, por exemplo.

Gestão de Riscos

EDUCAR PARA TRANSFORMAR

Riscos, medidas de segurança e o ciclo de segurança.

Barreira 05: Deter

Esta barreira representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, são bons exemplos.

Gestão de Riscos

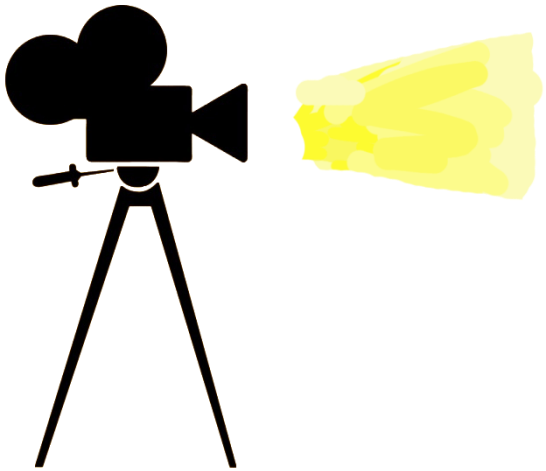
EDUCAR PARA TRANSFORMAR

Riscos, medidas de segurança e o ciclo de segurança.

Barreira 06: Diagnosticar

Apesar de representar a última barreira no diagrama, esta fase tem um sentido especial de representar a continuidade do processo de gestão de segurança da informação. Cria o elo de ligação com a primeira barreira, criando um movimento cíclico e contínuo. Devido a estes fatores é a barreira de maior importância. Deve ser conduzida por atividades de análise de risco que consideram tanto os aspectos tecnológicos quanto os físicos e humanos.

Vídeo: Truque de Mestre



(A Melhor Cena do Filme: Truque de Mestre: O Segundo Ato, disponível em: (https://www.youtube.com/watch?v=pZcF4oZbB14)).

Turma 1001 – continuar desse ponto 04/04