

Gestão da Tecnologia da Informação

Auditoria e Segurança da Informação

Francisco José Tosi



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Semana 4

Aula 07/08

Mitigando os riscos de
segurança

31/08

Francisco José Tosi



EDUCAÇÃO
METODISTA



Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Controles.

São medidas técnicas ou administrativas que evitam, neutralizam ou minimizam perdas ou indisponibilidades devido a ameaças ao risco da segurança da informação.

São referenciados em todo o momento da segurança da informação, porem raramente são definidos.



É importante definir os controles, técnicos, administrativos, pessoais.

Preventivos, de detecção e de compreensão corretiva.

Auditoria e Segurança da Informação

Mitigando os riscos à segurança

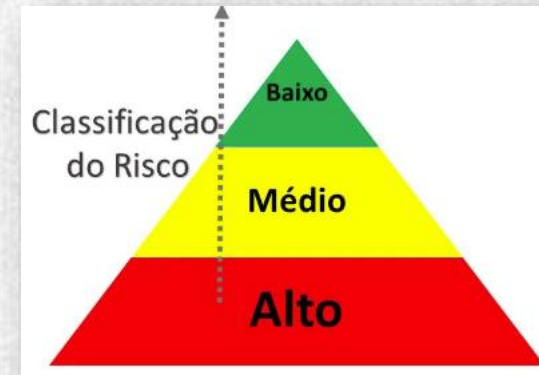
Considerando o tratamento de um Risco.

Deve ser definido o critério para determinar se o risco pode ou não ser aceito.

O risco pode ser aceito se for considerado baixo, ou o custo do tratamento for alto.

As decisões devem ser tomadas para cada risco existente

As decisões devem ser sempre registradas.



Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Possíveis controles para tratamento de riscos.

Deve ser definido o critério para determinar se o risco pode ou não ser aceito.

Aplicar: os controle adequados para reduzir o risco.

Aceitar: de forma consciente e objetiva os riscos, devem satisfazer as políticas e os critérios de aceitação do risco da organização.

Evitar: as ações que possibilitem a ocorrência do risco.

Transferir: para associados ou parceiros (seguradoras, fornecedores).



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Possíveis decisões para tratamento de risco.

Deve ser definido o critério para determinar se o risco pode ou não ser aceito.

Selecionar e implementar ações para atender ao requisitos identificados na avaliação do risco.

Assegurar que os riscos foram reduzidos a um nível aceitável, estando atento em obedecer critérios:

- Requisitos e restrições da legislação nacionais e internacionais.
- Objetivos organizacionais.
- Requisitos e restrições operacionais.
- Custo de implantação e operação em relação aos impactos ocasionados.



Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Contramedidas para mitigar o risco.

Na análise de risco é gerado lista de ameaças e suas importâncias.

Analisar cada ameaça e encontrar uma ou mais ações para reduzir as ameaças.

- ✓ Reduzir as chances do evento de risco ocorrer.
- ✓ Minimizar as consequências caso o risco ocorra.
- ✓ Uma combinação das duas.



Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Categoria das ações.

Como definir um plano de Ação?

As medidas devem ser criadas com base na análise de risco.

Preventivas: Visam evitar incidentes

Redução: Visam diminuir a probabilidade de ocorrer

Deteção: Visam detectar os incidentes

Repressivas: Visam limitar o incidente

Corretivas: Visam recuperação dos danos causados

Aceitar: não fazer nada



Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Prevenção.

Tornar impossível da ameaça ocorrer

Objetivo é tornar impossível da ameaça ocorrer.

Desconectar a internet e conectar à rede local evitando ação de *hackers*.

Fechar portas para impedir acesso de pessoas.

Institucional zonas de segurança em lugar onde a informação sensível possa ser mantida segura.

Colocar informações sensíveis em cofre após expediente.

Vigilância por vídeo, com adesivos informando que o ambiente é monitorado.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Prevenção.

Controle de alterações em sistemas

Garantir que alterações em um produto ou sistema são implantados de forma controlada e coordenada



Gerencia de mudanças.

Reduz a possibilidade de alterações desnecessárias sejam implantadas em um sistema sem permissão.

Reduz a possibilidade de implantação de sistemas com falhas, minimizando interrupções.

Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Detecção.

Pode ser utilizado quando as consequências diretas do incidente não são grandes ou existe tempo para minimizar o impacto esperado.

Os incidentes devem ser detectado o mais rápido possível.

Informar que o uso da internet é monitorado pode coibir a navegação indesejada.

Controlar o uso da internet pode coibir o uso improprio.



Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Repressão.

Quando o monitoramento aponta uma irregularidade, uma ação deve ser realizada.

A ação deve ser realizada para minimizar as consequências.



Fazer um *backup* é uma ação repressiva.

O backup pode ser utilizado para restaurar uma versão de armazenamento do documento.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Correção / Restauração.

Quando os incidentes deve ocorrer recuperação do que foi afetado.

A extensão do dano causado vai depender das medidas repressivas adotadas.



Quanto mais velho for o *backup* maiores serão os danos ocorridos.

Um sistema de *stand-by* é uma medida de corretiva.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Seguro.

Existem eventos que não podem ser prevenidos e as consequências são aceitáveis.

Para isso busca-se métodos para aliviar as consequências.

Um seguro de incêndio alivia as perdas financeiras causadas pelo incêndio.



Armazenar uma cópia de toda informação importante fora da organização garante que informações não serão perdidas em caso de incêndio.

Auditoria e Segurança da Informação

Mitigando os riscos à segurança

Aceitação.

Quando os riscos são necessários e conhecidos.

Pode-se decidir aceitar correr o risco.

Os custos pode ser muito alto, não compensando atuar no risco.

Pode não ter uma ação adequada para mitigar o risco.

A ação não é eficiente.

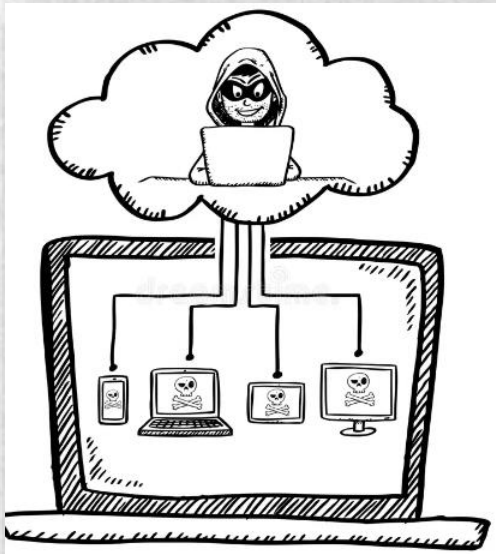


Auditoria e Segurança da Informação

Tipos de Ameaças

Ameaça humana Intencional.

Pode ser causadas por intrusos - *Hacker*.



Funcionário destruindo dados.

Venda de dados para a concorrência.

A ação não é eficiente.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Tipos de Ameaças

Ameaça Humana Intencional.

Engenharia Social busca explorar a falta de consciência sobre segurança na organização.

Um Engenheiro Social tira proveito de pontos fracos das pessoas para concretizar seus objetivos.

Se o *helpdesk* liga para perguntar onde está um determinado arquivo, deve existir a conscientização que sempre deve se certificar que a pessoa é do *helpdesk*



Falar sobre assuntos confidenciais de trabalho em público.

Auditoria e Segurança da Informação

Tipos de Ameaças

Ameaça Humana Não Intencional.

Os danos podem ser causados não intencionalmente.



Pode ser acionado um comando errado.

Pode abrir um e-mail ou inserir um *pen drive* com vírus

Sem conhecimento pode se utilizar um extintor de incêndio errado e danificar um servidor.

Auditoria e Segurança da Informação

Tipos de Ameaças

Ameaça Não Humana.

São eventos externos: Raios, incêndios, inundações, tempestades

Os danos depende da localização dos equipamentos.



A sala do servidor está localizada diretamente sob um telhado plano suscetível a vazamento?

Está localizado em subsolo onde pode ter umidade?

São situações tem influência no risco que a organização pode enfrentar



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Tipos de Danos

Dano direto: Furto, tem consequência diretas no negócio. Causado por água dos extintores de incêndio.

Dano indireto: é a consequência do que pode ocorrer. Ser incapaz de atender um contrato devido à infraestrutura de TI ser destruída pelo fogo.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Tipos de Estratégia de Risco

Tolerância ao risco: Certos riscos são aceitos, acontecem quando o custo da ação do risco é maior que o dano causado.

Também pode ser aceito pela administração mesmo que o custo das ação seja menor que o dano.

Redução (mitigação): São medidas para que o dano da ocorrência das ameaças sejam minimizadas.


A maioria das medidas tomadas pelas organizações que neutraliza o risco é uma combinação de medidas preventivas, de detecção e repressivas.

Prevenção (evitar): São medidas para a ameaças sejam neutralizadas, sendo que não leva mais a um incidente.

Atualização de software de um sistema operacional.



Auditoria e Segurança da Informação



springbooks

Estudo de Caso

Springbooks:

Fundada em 1901, durante a sua expansão para uma organização internacional que opera na Europa.

A empresa teve que mudar e se ajustar ao seu ambiente, foi a grande mudança ocorrida ao longo dos 50 anos no fornecimento de informações.

Há uma grande diferença de processos entre a época que a empresa foi fundada 1901, com surgimento da tecnologia e de comunicações (TICs), durante as décadas de 60 e 70 até os dias de hoje. As TICs se tornaram uma das mais importantes ferramentas da **Springbooks**.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

springbooks

Estudo de Caso

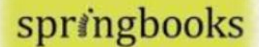
Springbooks:

A Springbooks é uma livraria que opera na Europa, com uma organização de 120 livrarias, a maioria funcionando com base em franquias, onde um total de 50 lojas permanece à própria empresa.

Henry Spring criou em 1901 uma pequena loja em Bedrock-on-Thames, Reino Unido.



Auditoria e Segurança da Informação



springbooks

Estudo de Caso

Springbooks:

Ao longo do tempo 36 lojas foram criadas nas principais cidades do Reino Unido.

Após a segunda guerra criou lojas em Amsterdã, Copenhague, Estocolmo, Bonn, Berlim e Paris.

Atualmente possui lojas em todas as principais cidades da União Europeia.

O conselho de diretores fica em Londres, A sede Europeia fica em Amsterdã, e todo país possui escritório central.

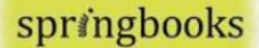
Todas livrarias pretão conta ao escritório Central.

Todas livrarias pretão conta ao escritório Nacional.

O escritório Nacional presta conta à sede europeia em Amsterdã.

A sede europeia presta conta ao Conselho de Diretores em Londres.

Auditoria e Segurança da Informação



springbooks

Estudo de Caso

Springbooks:

A Área de TI é organizada de forma centralizada.

Existe uma *Wide Area Network* (WAN) na qual todas as lojas estão conectadas.

A livrarias estão conectadas as *Local Area Network* (LANs) que são limitadas a uma única edificação.

As caixas registradoras são conectadas a WAN), todo livro vendido é escaneado na caixa registradora em uma base de dados central.

Todo funcionário possui seu próprio ID, que é utilizado para fazer login no sistema das caixas registradoras.

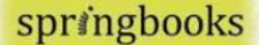
Todo livro vendido é associado ao colaborador que efetuou a venda.

Na base de dados existe muitas informações de clientes.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação



springbooks

Estudo de Caso

Springbooks:

A Springbooks possui uma organização de segurança da informação parcialmente centralizada, a principal maneira de tratar de segurança de informação é através da sede de Londres.

Em Londres há um Gerente Corporativo de Segurança da Informação, com responsabilidade de organizar a segurança da informação da empresa, e garantir que a segurança da informação seja parte do trabalho diário de todos colaboradores.

Fica a cargo dos escritórios garantir o cumprimento das leis e dos reguladores.

O encarregado da Segurança da Informação Local do país é responsável pela adesão às regras centrais e nacionais. Também é responsável pela segurança física das livrarias

Toda livraria possui um local de segurança da informação, que é um funcionário responsável pela segurança da informação das livrarias

Auditoria e Segurança da Informação



Atividade 3

Até agora a Springbooks só tinha implementado algumas medidas de segurança através de aplicações da melhores práticas em resposta a incidentes de segurança.

Porém o conselho da Springbooks decidiu que segurança será a parte de uma devida diligencia de segurança, e SEU GRUPO, terá que apontar a abordagem e as soluções para implantar a segurança da informação na Springbooks.

Identifique os riscos mais importantes à segurança com que a Springbooks terá que lidar.

Pense em Disponibilidade, Confidencialidade e Integridade. Em análise de risco

O sistema de pedidos da Springbooks está concentrado em um grande centro de computadores próximo de Londres. Esse centro de computadores é de propriedade de uma grande empresa de TI. A Springbooks terceirizou sua TI para essa empresa.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação



Dias Claudia; Segurança e Auditoria da tecnologia da informação Claudia Dias Indaial : Editora Axcel Books, 2000

Gross, Christian Meinecke; Segurança em tecnologia da informação / Christian Meinecke Gross; Jan Charles Gross. Indaial : Uniasselvi, 2013.

Hintzbergen, Julie; Fundamentos de Segurança da Informação: Com base nas normas ISO 27001 e na ISO 27002 / Julie Hintzbergen, Kees Hintzbergen, André Smulders, Hans Baars; Tradução Alan Sá – Rio de Janeiro : Brasport, 2015

Imoniana, Joshua Onome; Auditoria de Sistemas de Informação / Joshua Onome Imoniana; 2. ed. – 2. reimpr; S;ao Paulo : Atlas, 2010

Lyra, Maurício Rocha; Governança da Segurança da Informação / Edição do Autor, 2015

Sêmola, Marcos; Gestão da Tecnologia da Informação: visão executiva da segurança da informação : aplicada a Security Officer / Marcos Sêmola e Módulo Security Solutions S.A. Rio de Janeiro : Elsevier, 2003 – 10ª reimpressão

Silva, Michel Bernardo Fernandes da, Cibersegurança uma visão panorâmica sobre segurança da informação na internet / Michel Bernardo Fernandes da Silva. – Rio de Janeiro : Freitas Bastos, 2023.



EDUCAÇÃO
METODISTA