Gestão da Tecnologia da Informação

Auditoria e Segurança da Informação

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Semana 3

Aula 05/06

Avaliação de risco de segurança

23/08

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Segundo ISO 27005.

É o processo de planejar, organizar, conduzir e controlaras atividades visando minimizar os efeitos do risco sobre o capital e o lucro da organização.

Riscos podem surgir de várias maneiras:

Incerteza do mercado financeiro;

Falhas em projetos;

Responsabilidades legais;

Risco de crédito;

Acidentes;

Causas naturais e desastres;

Ataques de adversários.

Hintzbergen, 2015, p. 35

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Segundo ISO 27005.

Existem diversos padrões de gerenciamento de risco que variam muito:

Project Management Institute (PMI):

National Institute of Science and Techonology (NIST);

Padrões ISO.

Hintzbergen, 2015, p. 35

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Eliminar: Eliminar a ameaça eliminando a causa. Remover em 100% a probabilidade que a ameaça ocorra. Exemplo: cancelar o projeto.

Mitigar: Reduzir a probabilidade ou o impacto de uma ameaça, tornando-a um risco menor.

Transferir: Tornar outra parte responsável pelo risco contratando seguros, bônus de desempenho, garantias ou terceirização de trabalho. transferir total ou parcial o impacto em relação a uma ameaça para um terceiro. Exemplo: fazer um seguro.

Aceitar: A aceitação de ameaças reconhece a existência de uma ameaça, mas nenhuma ação proativa é tomada. Aceitar ativamente um risco pode incluir o desenvolvimento de um plano de contingência que seria acionado se o evento ocorresse; ou pode incluir aceitação passiva, que significa não fazer nada

Hintzbergen, 2015, p. 35

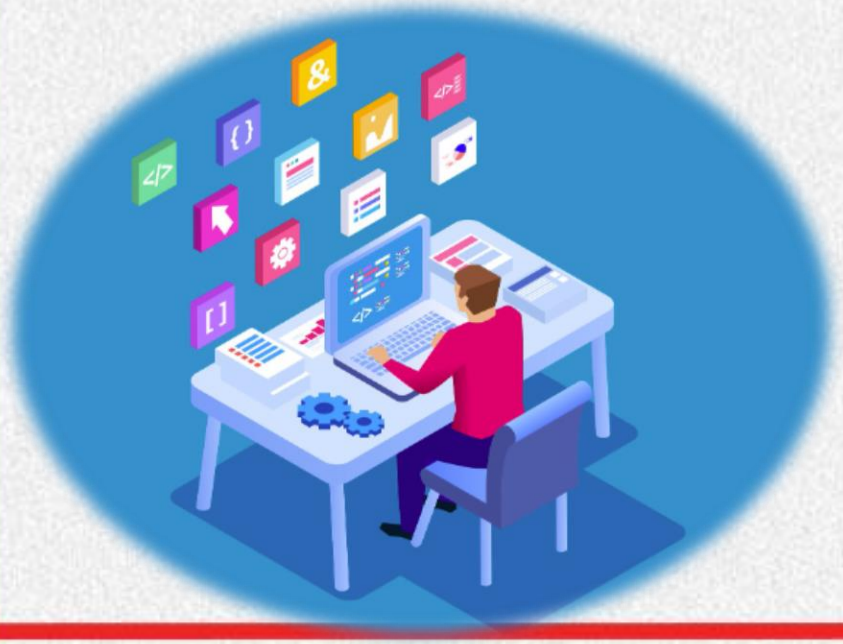
EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Gerenciar Risco: É o processo continuo que se aplica a todos os aspectos dos processos operacionais.

Em grandes organizações esse processo é coordenado e acompanhado por um especialista.



Chefe da segurança da informação.

Hintzbergen, 2015, p. 36

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Requisitos da segurança da informação:

Avaliação dos riscos da organização: leva em conta a estratégia e os objetivos globais de negócio.

As ameaças aos ativos devem ser identificadas.

A vulnerabilidade e probabilidade de ocorrência devem avaliadas.

Identificando o impacto.

EDUCAÇÃO METODISTA

Hintzbergen, 2015, p. 36

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Requisitos da segurança da informação:

Requisitos legais: são determinados por estatutos, regulamentos e contratos que uma organização tem que satisfazer.

A organização deve se preocupar que seus parceiros comerciais, contratantes e provedores de serviço também satisfaçam quando em seu ambiente socio cultural.

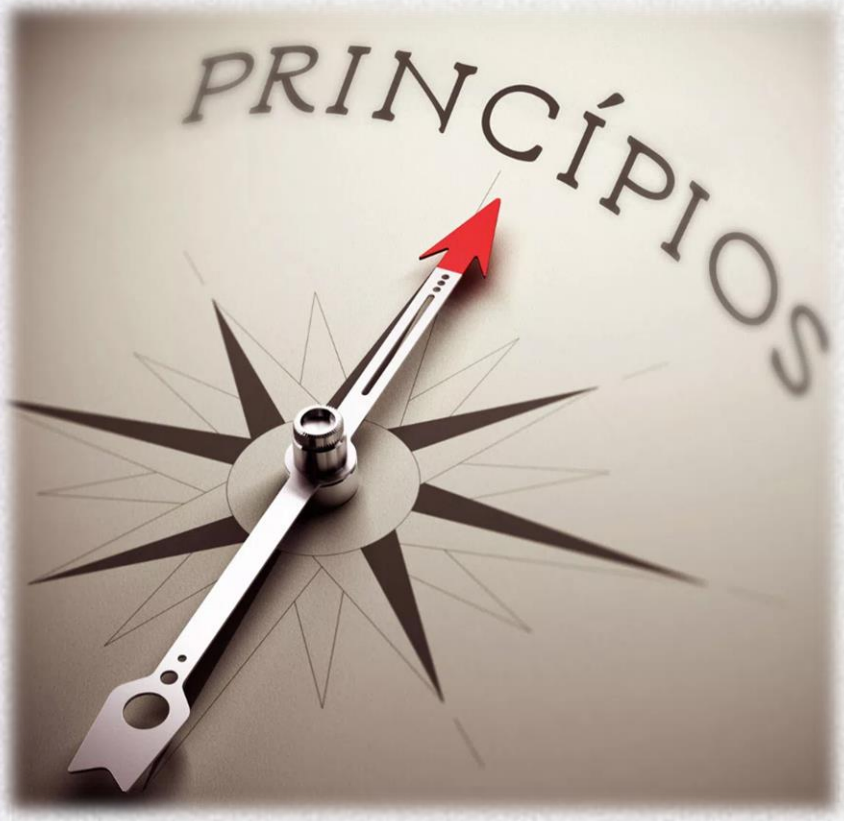
Hintzbergen, 2015, p. 36

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Requisitos da segurança da informação:



Conjunto de princípios: requisitos de negócios para manuseio, processamento, armazenamento, comunicação e arquivamento da informação que a organização desenvolveu para apoiar suas operações.

Hintzbergen, 2015, p. 36

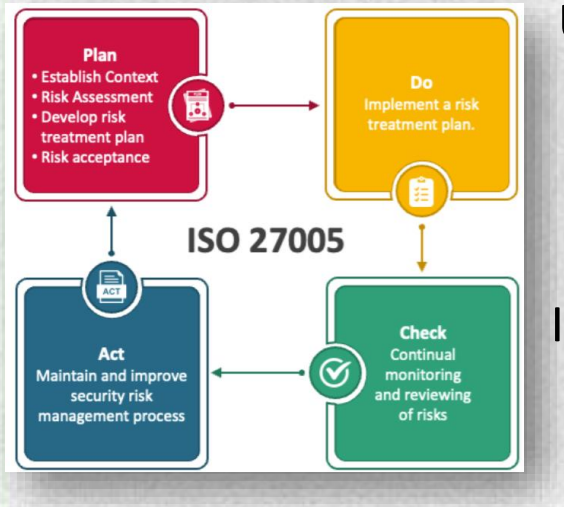
EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Requisitos da segurança da informação:

Devem ser empregados recursos equilibrados para controle dos requisitos de acordo com os prejuízos que podem ser gerados para a organização.



Uma boa avaliação do risco vai ajudar a guiar as ações e investimentos necessários e as prioridades de implementação de controles.

ISO 27007:2011 fornece orientações para gestão de risco de segurança da informação.

Hintzbergen, 2015, p. 37

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Avaliação do Risco:

A avaliação de risco da segurança deve ser conduzida nas primeiras etapas do projeto.

Deve identificar os controles necessários para a segurança da informação.

Deve iniciar no delineamento do projeto para alcançar o nível de segurança necessários .

Deve identificar e quantificar e priorizar os riscos.

Hintzbergen, 2015, p. 38

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Avaliação do Risco:

A avaliação deve incluir uma abordagem sistemática ao tamanho dos riscos.

Avaliação de riscos devem acontecer periodicamente para tratar de mudanças nos requisitos de segurança da informação

Deve ter um âmbito claramente definido, a fim de ser eficaz, incluindo avaliações de risco de outras áreas.

Hintzbergen, 2015, p. 38

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Abordagem sobre Análise de Risco segundo ISO 27005:

Análise de risco é processo de definir e analisar os perigos pelos quais indivíduos, empresas e agências governamentais passam em decorrência de potenciais eventos adversos naturais ou casados pelo homem.

O objetivo de realizar a análise de risco é esclarecer quais ameaças são relevantes para os processos operacionais e identificar os riscos associados.

Serve para determinar o nível de segurança apropriado e as medidas de segurança que devem ser adotadas.

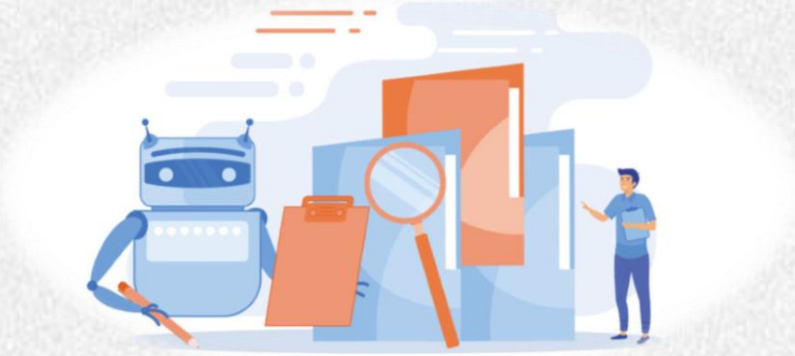
Serve para garantir que as medidas de segurança sejam implantadas de forma econômica eficiente e eficaz.

Hintzbergen, 2015, p. 38

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Abordagem sobre Análise de Risco segundo ISO 27005:



Objetivos principais de uma análise de risco.

- ✓ Identificar os ativos e seus valores.
- ✓ Determinar as vulnerabilidades e ameaças.
- ✓ Determinar os riscos de ameaças se tornarem realidade e interromperem os processos operacionais.
- ✓ Estabelecer equilíbrio entre os custos de um incidente e os custos de uma medida de segurança.

EDUCAÇÃO METODISTA

Hintzbergen, 2015, p. 39

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Análise quantitativa dos riscos:

Calcular com base no impacto do risco.

O nível financeiro e a probabilidade de uma ameaça se tornar um incidente.

Pode ser composto por custos das medidas de segurança, valor do estabelecimento e impactos nos negócios.

É possível ter uma imagem clara do risco financeiro total e as medidas adequadas que podem ser determinadas.

Hintzbergen, 2015, p. 40

Auditoria e Segurança da Informação

Avaliação de risco de segurança – Gerenciamento do Risco

Análise qualitativa dos riscos:

Valores monetários que serão atribuídos a componentes e perdas.

Classificam a gravidade da ameaça.

Incluem o bom senso, melhores práticas, intuição e experiencia.

Ex. Delphi, *brainstorming*, grupo de discussão, pesquisas, questionários, lista de verificação.

EDUCAÇÃO METODISTA

Hintzbergen, 2015, p. 41

Auditoria e Segurança da Informação

Atividade 2

Realizar a **leitura individual** do artigo:

Acompanhe estas 7 tendências para segurança cibernética proativa em 2024

Disponível em: Track These 7 Trends for Proactive Cybersecurity in 2024 (isaca.org)

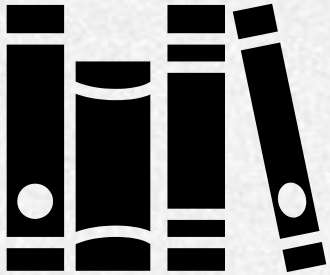
Em grupo debater sobre as questões, criar um documento com as conclusões do debate e disponibilizar no Moodle:

1. Devido ao aumento de sofisticação esperado nas ameaças digitais, uma alternativa é que os profissionais de cibersegurança utilizem a inteligência artificial para combater os ataques cibernéticos. Debata com seu grupo como a IA pode ajudar na segurança cibernética.
2. Estima-se que 36,2 milhões de pessoas nos Estados Unidos trabalharão remotamente até 2025. Debata quais os riscos que isso pode trazer, e por quê.
3. O número de aplicativos móveis vem aumento consideravelmente, debata quais os desafios que podemos ter com o aumento dos aplicativos móveis.
4. A internet das coisas está cada vez mais transformando objetos do cotidiano em dispositivos inteligentes e interconectados. Debata qual o risco que essa interconexão pode trazer.
5. As organizações estão reconhecendo os benefícios que o armazenamento em nuvem traz. Debata quais desafios de segurança cibernética quem existir em armazenamento em nuvem.
6. Ataques cibernéticos patrocinadas pelo estado tornam-se uma preocupação, debata quais são esses ataques e porque são preocupação.
7. Existe uma deficiência em encontrar talentos para tratar ataques cibernéticos. Debata quais são essas dificuldades

O Assunto abordado neste artigo será pedido em prova

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