Gestão da Tecnologia da Informação

Auditoria e Segurança da Informação

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Semana 6
Aula 11/12
Segurança Lógica

13/09

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Os problemas de segurança da informação são complexos, conforme Beal (2008), e normalmente têm sua origem em preocupações organizacionais e de negócio, não de tecnologia

Para garantir um nível de proteção adequado para seus recursos de informação, as organizações precisam ter uma visão clara

Dos ativos que estão tentando salvaguardar

Das ameaças

Qual o motivo

Gross, 2013, p. 55

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Pela área de Tecnologia de Informação transita grande número de informações sensíveis e estratégicas **para a empresa** e de **interesse de outras empresas**.

A divulgação de algumas dessas informações pode ocasionar prejuízos e penalidades graves

A **segurança lógica** compreende a integridade dos ativos de dados e dos programas da empresa

Gross, 2013, p. 55

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Problemas de segurança se multiplicam.

Usuário com um microcomputador ou laptop se transforma num “administrador de sistema”,

Uma série de procedimentos de segurança precisam ser gerenciados

A **segurança lógica** trabalha estabelecendo mecanismos de acesso a arquivos, sistemas e páginas Web da empresa, limitando a disponibilidade de recursos para cada usuário

Gross, 2013, p. 56

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança

Após definição das Políticas de Segurança

Definir a Estrutura da Administração da Segurança

Tipo da Estrutura

Localização dentro da estrutura da organização

Perfil do profissional

Diretrizes da segurança

Ferramentas Administrativo e Técnico

Grau de padronização

Gross, 2013, p. 56

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Estrutura da administração da segurança

Assume as tarefas de segurança do ambiente de informações

Físico e Lógico

Tipo da Estrutura

Definir claramente o seu domínio de atuação, a autoridade e as regras sobre as quais se basearão suas atividades

Gross, 2013, p. 57

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Tipos de Estrutura

Deve ser definido o tipo de estrutura de administração da segurança entre **centralizada ou descentralizada**

Não existe uma resposta pronta para escolha

Pode existir uma resposta certa em relação a um **ambiente individual**

Uma cuidadosa análise de cada ambiente de informações pode determinar qual será a melhor resposta

EDUCAÇÃO METODISTA

Gross, 2013, p. 57

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Tipos de Estrutura

Centralização

Vantagens	Desvantagens
✓ Maior simplificação organizacional e de procedimentos	✗ Menor grau de flexibilidade
✓ Especialistas de segurança dedicados	✗ Desconhecimento de condições locais
✓ Menor dispersão de esforços	✗ Custo maior concentrado em uma única área
✓ Menor sobreposição de estruturas de segurança	✗ Tempo de resposta mais lento
✓ Maior rapidez de manutenção	

Gross, 2013, p. 58

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Tipos de Estrutura

Descentralização

Vantagens	Desvantagens
✓ Maior flexibilidade	✗ Aumento da burocracia
✓ Manutenção local mais rápida	✗ Maior sobreposição de estruturas de segurança
✓ Maior familiaridade com as exigências locais	✗ Menor conhecimento da segurança
✓ Responsabilidade e relacionamento distribuídos	✗ Maior suscetibilidade a pressões locais
	✗ Maiores dificuldades de controle por parte da auditoria ou outro órgão de controle

Gross, 2013, p. 58

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Tipos de Estrutura

"A segurança descentralizada distribui o esforço de manutenção da segurança, de forma que a função não se torne um ônus para apenas uma área. Além disso, a manutenção poderá ser subordinada a uma área que pode ter um conhecimento maior e mais adequado dos recursos que serão protegidos. Porém, haverá um esforço adicional na área central para controlar as atividades dos administradores descentralizados."

Caruso e Steffen (1999, p. 106),appud Gross

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Tipos de Estrutura

Aspectos para decidir quem será o responsável pela administração da segurança:

- ✓ tamanho de cada organização
- ✓ as instalações de processamento de informações
- ✓ atividades de manutenção necessárias

Gross, 2013, p. 59

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Tipos de Estrutura

- ✓ Do número de entidades hierárquicas e ferramentas envolvidas, ou seja, departamentos, divisões, aplicações etc.
- ✓ Do número de usuários definidos, e dos requisitos de movimentação de empregados.
- ✓ Da quantidade de recursos que devem ser protegidos.
- ✓ Da existência de padrões.
- ✓ Dos diferentes tipos de recursos que devem ser protegidos e da extensão da segurança requerida para cada um destes recursos. Deve ser lembrado que a Internet pode exigir uma estrutura exclusiva de controle.

Gross, 2013, p. 58

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Tipos de Estrutura

- ✓ Do número de entidades que devem ser protegidas, o que pode implicar um trabalho de manutenção enorme em alguns casos.
- ✓ Das atividades de desenvolvimento de aplicações. Se a atividade de desenvolvimento for considerável, como é o caso da maioria das instalações, a revisão da segurança e das atividades de manutenção também devem ser consideradas.
- ✓ Dos requisitos de auditoria e da frequência de alterações destas.
- ✓ Do número de recursos definidos para os usuários e das atividades previstas para eles.
- ✓ Das ferramentas de segurança selecionadas. Cada uma difere das outras em função do volume de trabalho envolvido e do perfil necessário para a manutenção da segurança.

Gross, 2013, p. 59

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança - Localização da Segurança

É melhor que o administrador de segurança esteja envolvido desde o início da implantação da estrutura de segurança.

administrador será capaz de gerenciar as tarefas diárias e constantes.

O administrador de segurança deve ser alocado em algum lugar dentro da própria organização

o melhor lugar é onde a área de administração de segurança se relacione mais diretamente com a alta administração

Gross, 2013, p. 59

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança - Localização da Segurança

A área de segurança da informação não pode se torne menos suscetível a pressões e comprometimentos resultantes de lealdades para com a área funcional à qual a administração de segurança pertença.

Uma opção pode ser incluir todas as funções de segurança, compreendendo os requisitos de segurança física, dentro desta área evitando que exista estruturas similares na mesma organização.

Custo de uma estrutura pode ser muito alto para as organizações e faz com que administração de segurança deve residir em uma área onde tenha o poder de impor a segurança.

Gross, 2013, p. 59

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança - Localização da Segurança

"Indicam que bom é posicioná-la, pelo menos em termos de subordinação hierárquica, junto à estrutura de segurança empresarial, que cuida da segurança das organizações em um nível global, caso exista tal estrutura dentro da empresa."

"As organizações devem ter uma política de segurança global, voltada para a normatização e o controle. Essa normatização e controle não significam a centralização operacional".

Caruso e Steffen (1999, p. 109) appud Gross

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Perfil do Profissional de Segurança

O trabalho de um administrador de segurança é, sem dúvida, difícil

"A natureza da função forçará o administrador a se imiscuir em todos os "cantos escuros" da organização.

É uma posição de alta responsabilidade, que requer determinação e segurança por parte do profissional.

Gross, 2013, p. 59

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Perfil do Profissional de Segurança

Características

- ✓ Conhecimento dos recursos dos ambientes de informações e dos requisitos de segurança adequados.
- ✓ Alto grau de responsabilidade.
- ✓ Boa experiência organizacional e em análises.
- ✓ Sensibilidade para a política do ambiente de informações.
- ✓ Facilidade em se relacionar, pois a maior parte do trabalho envolve convencer as pessoas.
- ✓ Estabilidade emocional.

Gross, 2013, p. 59

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Perfil do Profissional de Segurança

Diz-se que um bom profissional de segurança deve ter coração de pedra e nervos de aço e ser insensível a ofensas e insultos.

CARUSO; STEFFEN, 1999, p. 110), apud Gross

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Diretrizes da Segurança

Definir as diretrizes da segurança no inicio

Devem estar definidas na política global de segurança da empresa, como parte das atribuições e responsabilidades que se espera que todos os empregados sigam

As diretrizes de segurança mais específicas devem ser formadas de normas à parte da política e devem se basear nas diretrizes gerais da política

não devem ser rígidas para que seja possível adequar às particularidades de cada caso

EDUCAÇÃO METODISTA

Gross, 2013, p. 61

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Diretrizes da Segurança

- ✓ Procedimentos padrões de segurança que serão utilizados no ambiente de trabalho na empresa.
- ✓ Documentação dos controles de segurança disponíveis para cada tipo de recurso e a comunicação a todos os envolvidos.
- ✓ Estimativa dos riscos e comprometimentos dentro do ambiente da empresa.
- ✓ Registro e relato das violações para as pessoas indicadas.

Gross, 2013, p. 61

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Diretrizes da Segurança

- ✓ Acompanhamento do desenvolvimento de requisitos de segurança para todos os projetos dos usuários.
- ✓ Treinamento de todos os usuários com relação à política de segurança da empresa.
- ✓ Se for necessário, apoio às administrações descentralizadas e seu controle.
- ✓ Responsabilização dos envolvidos com a função de segurança, desde o administrador central até o usuário final; deve ser dado um enfoque especial ao papel das áreas de informática em relação à segurança, já que é ali que se encontram as maiores vulnerabilidades.

Gross, 2013, p. 61

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Ferramentas Administrativo e Técnico

Uma boa parte dos procedimentos administrativos depende da definição de outros aspectos da segurança, como diretrizes globais e específicas da segurança, a estrutura e o tipo de estrutura utilizados, o tamanho da equipe, o produto de segurança a ser adotado, entre outros.

O ferramental administrativo é altamente dependente da cultura de cada organização enquanto que o ferramental técnico é dependente do produto de segurança adotado pela empresa.

Gross, 2013, p. 61

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Padronização

Padronização de nomenclatura é o tipo de atividade que todos acham necessária, mas que, frequentemente, vai sendo adiada indefinidamente.

Os produtos de segurança da informação são baseados no agrupamento de funções, portanto a implantação de procedimentos de segurança será mais facilmente executado se forem desenvolvidos padrões de nível global.

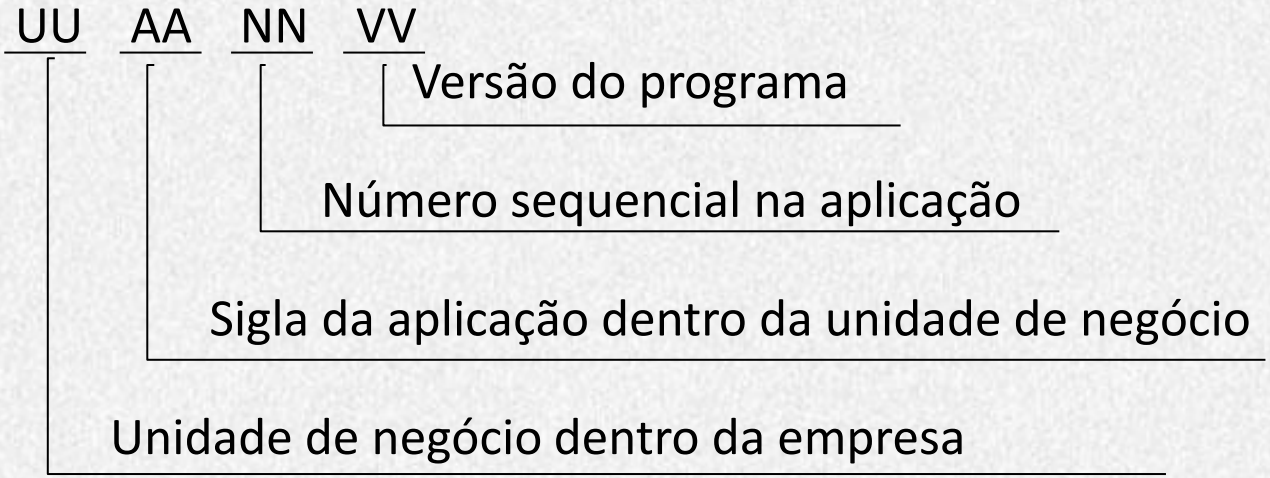
Gross, 2013, p. 61

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Padronização

Por exemplo: Padrões de nomes torna a criação de lista de acesso mais fácil.



O número de manutenção exigido por uma estrutura de segurança é inversamente proporcional ao grau de padronização existente dentro da organização

Gross, 2013, p. 62

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Equipe do projeto

O administrador de segurança, deve estar definido a esta altura, deve ser o coordenador da equipe.

Se a estrutura da administração de segurança já tiver sido implantada, é conveniente que pelo menos um dos integrantes participe da equipe, de preferência na função de relator e para providenciar os trâmites administrativos necessários.

Gross, 2013, p. 63

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Controles

As atividades administrativas necessitam de controles firmes

Devem ser definidos os controles necessários

Devem ser implantados após a escolha da ferramenta

- ✓ Domínio de usuários
- ✓ Domínio de recursos
- ✓ Integração entre os recursos

Gross, 2013, p. 63

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Controles da estrutura de segurança

Estrutura de Usuários

Estrutura hierárquica dos grupos de usuários;

Usuários de cada grupo;

Usuários com atributos especiais;

Recursos

Grupo de recursos protegidos;

Recursos de cada grupo;

Nível de proteção da cada grupo de recurso;

Nível de proteção da recurso individual;

Recursos com proteção especial;

Gross, 2013, p. 63

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Controles da estrutura de segurança

Integração de usuários versus recursos

Recurso que cada usuário pode acessar;

Usuários que acessam cada recurso;

Nível de acesso permitido a cada grupo / usuário;

Gross, 2013, p. 64

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Administração da Segurança – Controles sobre atividades de usuários

Violação de acesso a ambientes;

Violação de acesso à recursos;

Acesso a recursos monitorados;

Acesso de usuários monitorados;

Gross, 2013, p. 64

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Levantamento dos Recursos e de Usuários

Levantamento dos Usuários e Recursos;

Deve ser levantado as necessidades de cada grupo de usuários;

- ✓ Quem são os usuários?
- ✓ Quais são os recursos e como eles podem ser classificados?
- ✓ Quem é o responsável por cada recurso?
- ✓ Qual é o perfil atual de acesso a recursos?
- ✓ Qual é o perfil desejável de acesso a recursos?

Gross, 2013, p. 69

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Escolha de Ferramentas

A avaliação da ferramenta de segurança depende diretamente do ambiente global a ser protegido

As ferramentas de segurança, funcionam de forma sensivelmente diferente entre si, deve ser realizado um trabalho cuidadoso de avaliação

Montar uma planilha de avaliação que deve constar os quesitos que a ferramenta deverá possuir para atender a situações específicas existentes em cada um dos ambientes a proteger

Atribuir peso para cada item do conjunto de quesitos de avaliação, tendo como base a importância de cada quesito dentro do ambiente de informações

EDUCAÇÃO METODISTA

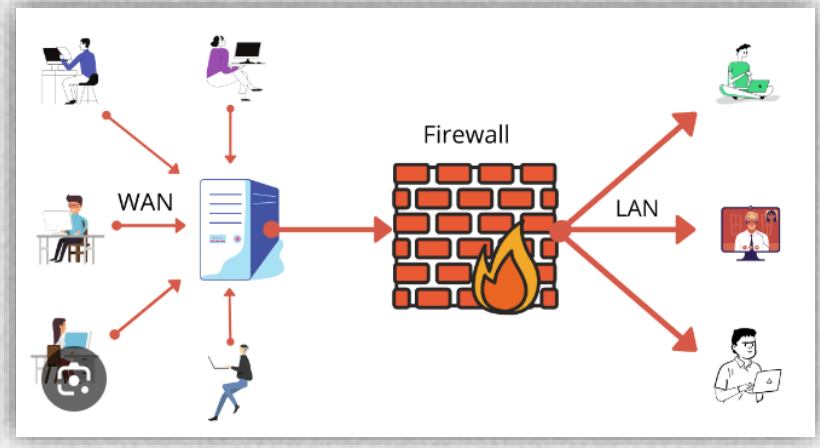
Gross, 2013, p. 70

Auditoria e Segurança da Informação

Segurança Lógica:

Escolha de Ferramentas

A segurança lógica também se beneficia de barreiras criadas em torno de um ativo ou conjunto de ativos de informação que se deseja proteger



- ✓ *firewalls* de rede
- ✓ mecanismos de controle de acesso
- ✓ dispositivos confiáveis de autenticação
- ✓ antivírus
- ✓ VPNs (redes privativas virtuais construídas sobre a infraestrutura de uma rede pública, geralmente a Internet)
- ✓ *bastion hosts (gateways* instalados entre uma rede interna e o ambiente externo para protegê-la de ataques)

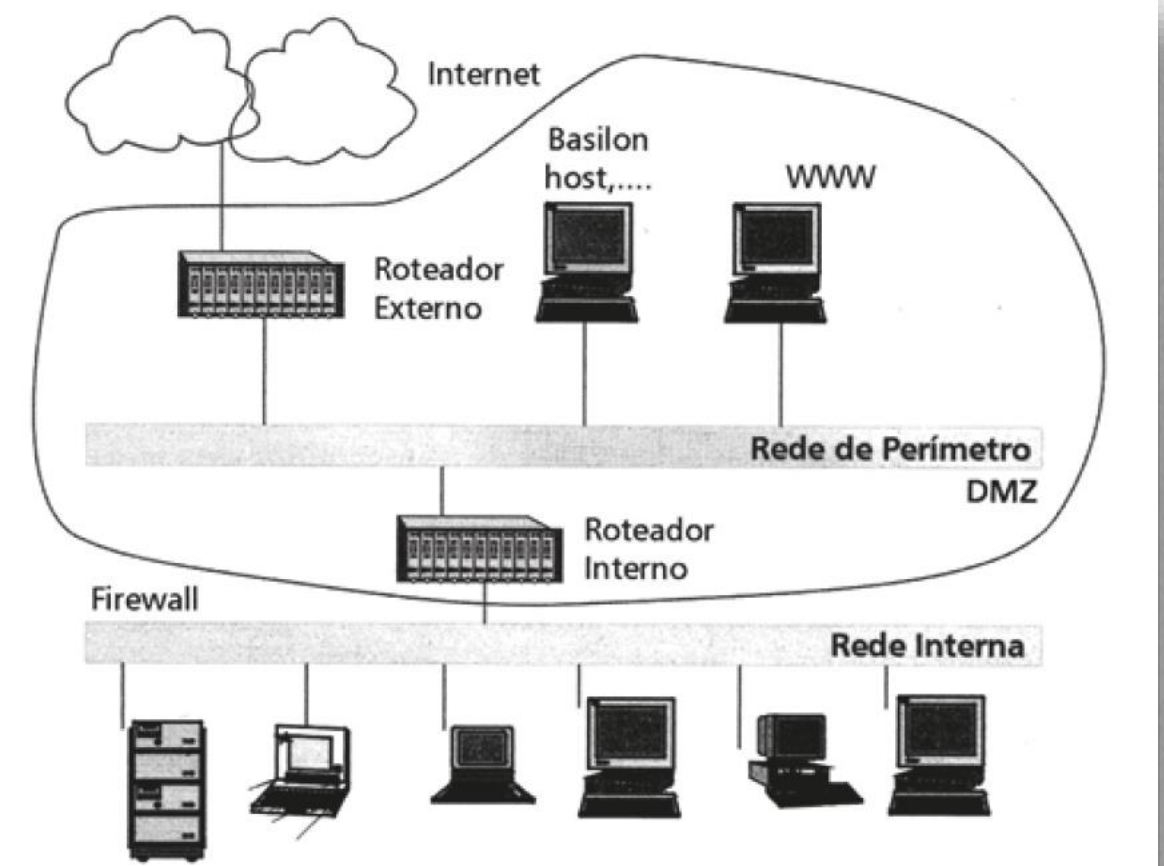
Gross, 2013, p. 71

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Escolha de Ferramentas



FONTE: Beal (2008, p. 96)

Gross, 2013, p. 71

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Comunicação de Dados e Criptografia

A criptografia é baseada em um mecanismo de conversão (o algoritmo de cifragem) que converte informações de texto claro para texto cifrado usando uma chave de cifragem conhecida somente pelo emitente e do receptor.

O mecanismo pode ser de conhecimento público ou até mesmo não ser conhecido por ninguém, mas as chaves usadas no processo nunca podem ser reveladas

Devido ao risco de decifração do texto e consequente dedução da chave, estas devem ser trocadas com frequência, o que implica a possibilidade de interceptação do meio usado para comunicar as chaves entre as partes.

Gross, 2013, p. 73

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Segurança para Micro, Terminais e Estações

Os equipamentos de microcomputação, terminais e estações de trabalho são menos exigentes em termos de condições ambientais que os grandes computadores.

Isso nem sempre é verdade, e não impede que os mesmos recebam tratamento de segurança similar ao dado a grandes computadores e seus periféricos.

O grau de proteção dependerá somente da importância que esses equipamentos tiverem para o desenvolvimento dos negócios da organização e não somente do porte e complexidade dos equipamentos.

Gross, 2013, p. 71

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Lógica:

Segurança em Redes

Não há como garantir segurança absoluta em qualquer tipo de rede com acesso ao público ou conectada à internet

Uma boa ação é a do Menor privilégio possível. O que não é explicitamente permitido, é proibido.

Gross, 2013, p. 75

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Atividade 4

Realizar a **leitura individual** do artigo:

Compreendendo e mitigando o risco da IA versus software tradicional

Disponível em: Entendendo e mitigando o risco de IA versus software tradicional (isaca.org)

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

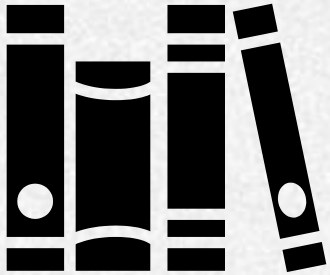
1. O artigo inicia comentando "*O uso de inteligência artificial (IA) ganhou um impulso considerável recentemente, especialmente com o lançamento do chatbot ChatGTP da OpenAI A IA tornou-se mais acessível e está agora a transformar a forma como as pessoas trabalham, comunicam e tomam decisões*". Qual a opinião do seu grupo quanto à essa afirmação?
2. Segundo o artigo são muitas e diferentes as percepções do IA. Qual a percepção do seu grupo referente a IA?
3. O artigo aborda que, assim como existe riscos em sistemas, existem riscos específicos em IA, como seu grupo vê esse assunto e quais riscos vocês entendem que são mais importantes?
4. A "*expicalibildade*" é um item que deve ser bem observado na utilização do IA, debata sobre essa dificuldade de "*explicabilidade*" existente no IA.
5. O IA pode ter problemas de preconceito, qual a opinião do seu grupo sobre isso, e como podemos evitar isso?

Conforme o artigo a robustez refere-se à capacidade de suportar desafios, o IA pode cometer erros. O que seu grupo entende por esses desafios?

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