

Gestão da Tecnologia da Informação

Auditoria e Segurança da Informação

Francisco José Tosi



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Semana 2

Aula 03/04

Definições para a
Segurança da Informação

16/08

Francisco José Tosi



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Como todos nós já sabemos, Tecnologia da Informação é fundamental para a operação das empresas.



Sabemos também necessidade de se preservar os sistemas dos ataques de hackers e as informações dos vazamentos não autorizados.

É importante a conscientização da necessidade de se tratar a segurança da informação no nível estratégico das organizações e não deixar essa tarefa apenas para as equipes técnicas especializadas.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

De uma forma simples e direta, a Informação pode ser definida por um conjunto de dados tratados e organizados de tal maneira que tragam algum significado ou sentido dentro de um dado contexto.

Se profissional de alguma Área falar a palavra “**Segurança**”.

A princípio, tal palavra não traz nenhum sentido ao profissional ao receptor da mensagem.

Não há um contexto; Não há um significado.

Portanto, até o momento, a palavra “**Segurança**” representou apenas um dado qualquer, um dado bruto, um fato, um elemento não interpretado.

Auditoria e Segurança da Informação



A palavra **SEGURANÇA** tem por natureza uma sensação **negativa**

Ela é aplicada por um motivo
**QUANDO HÁ RISCOS DAS COISAS
NÃO OCORREREM COMO DEVERIAM**



**EDUCAÇÃO
METODISTA**

Auditoria e Segurança da Informação

Mensagem for da seguinte forma “**Estudo Segurança da Informação**”.

Perceba que desta maneira, o profissional receptor da informação será capaz de compreender a mensagem.

Portanto, a presença de um contexto definido (neste caso, o contexto da segurança da informação) e da organização e tratamento dos dados não interpretados (estudar, segurança e informação) trouxe um sentido (significado) para a frase.

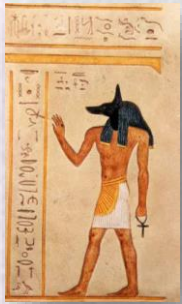


A segurança de TI é
RESPONSABILIDADE DE TODOS muitos
usuários de TI não sabem Disso

Auditoria e Segurança da Informação

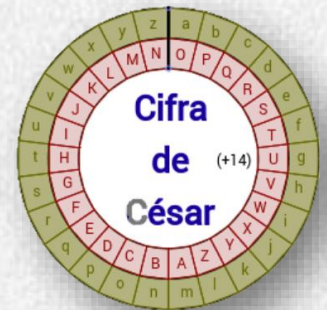
As raízes da **SEGURANÇA de TI** tem mais de 2.000 anos de idade

Como isso é possível?



Os egípcios utilizam hieroglifos esculpidos em monumentos e

Os romanos inventaram os chamados cifra de César para criptografar mensagens



Segurança física também é antiga – Muralhas da China



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação



Nos últimos anos a segurança física está cada vez mais dependente de TI

A segurança Física também é necessária para proteger a informas

Ambas estão juntas

Auditoria e Segurança da Informação

A necessidade de as informações passou a ser crucial para estas organizações.

Que empresa quer que suas estratégias de negócio sejam vistas pelos seus concorrentes?

Que executivo, em um momento de decisão de compra de uma determinada empresa, gostaria de ter sua informação manipulada e alterada?

A falta de uma correta abordagem da segurança da informação pode trazer altíssimos prejuízos para uma empresa.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Estratégia para Segurança da Informação

Para se estabelecer o grau de importância para as informações, que existem dentro de uma organização, é necessário avaliar o dano que a sua perda, ou o seu vazamento, poderá provocar para a operação ou para os negócios.

A análise deve ser realizado no planejamento estratégico da empresa.

etapa de diagnóstico: onde é analisada criticamente a situação atual da organização em relação aos objetivos propostos anteriormente

etapa de prospecção: nessa etapa são desenhados os cenários futuros para o ecossistema da organização e estabelecidos novos objetivos estratégicos para os próximos anos

etapa de elaboração de planos: os objetivos estratégicos estabelecidos são desdobrados em planos de ações para cada área de organização. Os planos de ações receberão metas objetivas e orçamentos necessários

Auditoria e Segurança da Informação

Sensibilidade da Informação

Nível 1 – Informação pública – informação que foi obtida sem ônus, de fontes públicas, ou que foi produzida internamente pela empresa mas que tem interesse público, que não precisam de controle de acesso e de distribuição.

Informações que devem apenas serem cuidar para que não sejam danificadas ou alteradas.

Exemplo:

Dados do balanço de empresas de capital aberto;

Lista de produtos;

Notícias sobre a empresa.



Auditoria e Segurança da Informação

Sensibilidade da Informação

Nível 2 – Informação restrita - informação que foi adquirida de terceiros com cláusula de sigilo mas que outras empresas também podem adquirir, ou que foi produzida pela empresa e que tem interesse restrito à ela.

Se vazadas, podem comprometer a imagem da organização mas não sua operação.



Exemplos:

Relatórios de consultoria sobre empresas concorrentes

Dados pessoais dos funcionários e executivos da empresa

Relatos de defeitos de produtos e serviços

Auditoria e Segurança da Informação

Sensibilidade da Informação

Nível 3 – Informação sigilosa - informação que foi obtida, com exclusividade, de terceiros, ou que foi produzida pela empresa e que trata de decisões, processos ou produtos críticos para a sua operação.

Se vazadas ou danificadas, podem gerar decisões erradas e prejudiciais para a operação da empresa ou inviabilizar o lançamento de um novo produto ou serviço



Exemplos:

Relatórios de investigação de práticas concorrenciais ilegais

Detalhes sobre campanhas de lançamento comercial

Detalhes sobre planos de fusão, aquisição ou fechamento de empresas

Auditoria e Segurança da Informação

Sensibilidade da Informação

Nível 4 – informação secreta – informação referente a detalhes de produtos e serviços que estão em processo de desenvolvimento ou, decisões sobre significativas alterações do valor patrimonial da empresa.

Se vazadas ou danificadas, podem comprometer o protagonismo no lançamento de um novo produto ou ainda permitir que concorrentes o lancem antes da empresa



Exemplos:

Detalhes de produtos e serviços em desenvolvimento

Detalhes sobre a negociação de compra ou venda de empresas ou filiais

Relatórios sobre falhas graves, em produtos, serviços ou processos internos, que podem afetar o valor das ações da empresa na bolsa de valores



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Sensibilidade da Informação

Nível 5 – Informações ultra secretas– informações sobre atos e fatos da organização cujo acesso é limitado apenas à mais alta direção executiva e seus acionistas.

Se vazadas, podem levar a ações judiciais à empresa ou a seus executivos e acionistas. Informações sobre segredos industriais que diferenciam a empresa de seus concorrentes



Exemplos:

Detalhes sobre operações ilícitas ou de alto risco jurídico

Segredos industriais sobre componentes, insumos ou processos de produção dos principais produtos da empresa ainda não patenteados ou protegidos por lei



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Sensibilidade da Informação

As informações de níveis 1 e 2 não precisam ser tratadas pelo nível estratégico da empresa, bastando as salvaguardas tradicionais das áreas técnicas

As demais precisam ser consideradas no planejamento estratégico, pois sua guarda e proteção implicam em despesas significativas e riscos a serem mitigados e compartilhados pela alta direção

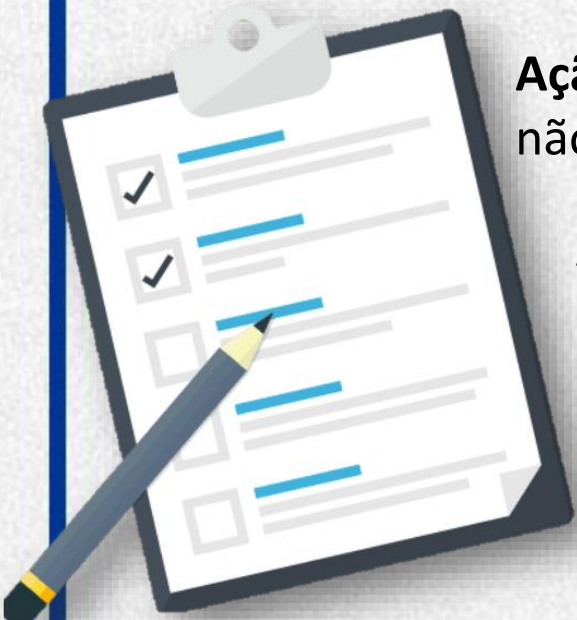
As informações de nível 5 devem ficar fora das redes corporativas (em computadores isolados) e, preferencialmente, não documentadas sob qualquer meio ou formato



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Definições para a Segurança da Informação



Ação preventiva: ação para eliminar a causa de uma potencial não conformidade ou outra potencial situação indesejável.

Aceitação de risco: não fazer nada em relação a exposição do risco.

Ameaça: causa potencial de uma situação indesejada, a qual pode resultar em dano a um sistema ou para a organização.

Análise da informação: proporciona uma clara imagem de como uma organização manuseia a informação e como a informação flui na organização.

Análise de riscos : processo para compreender a natureza do risco a fim de determinar o seu nível.

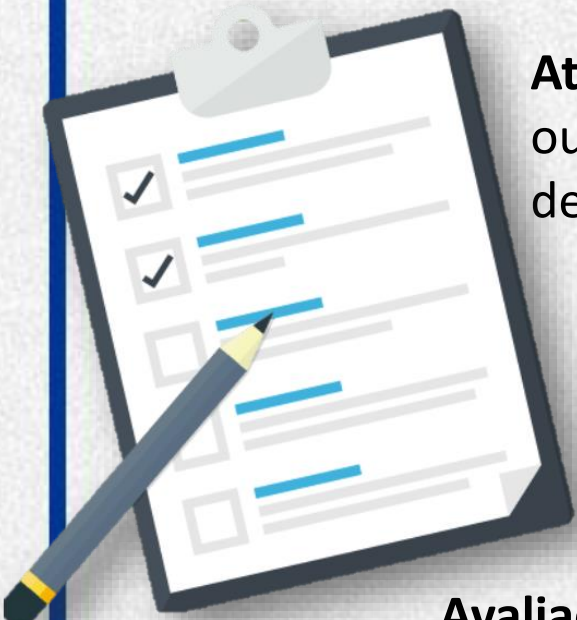
Proporciona a base para a estimativa do risco para as decisões sobre as ações a serem tomadas, essa análise inclui estimativa do risco.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Definições para a Segurança da Informação



Ataque: tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a, ou fazer uso não autorizado de um ativo.

Ativo: qualquer coisa que tenha valor para a organização (instalações, informações, software, hardware, serviços impressos-papeis, pessoas, habilidades, experiência, reputação e imagem).

Avaliação de risco: avaliar o risco e o processo geral de identificação do risco, análise do risco e estimativa do risco.

Confiabilidade: consistência dos comportamentos dos resultados desejados.

Confidencialidade: propriedade em que a informação não é disponibilizada ou divulgada as pessoas, entidades ou processos não autorizados.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Definições para a Segurança da Informação

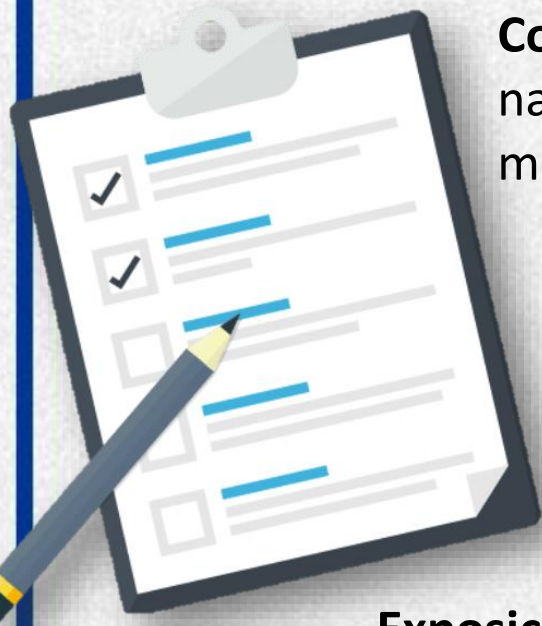
Controle: maíor e gerenciar o risco, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modifiquem o risco à segurança da informação.

Eventos de segurança da informação: ocorrência identificada de um estado de sistema, serviço ou rede que identifique uma possível violação da política de segurança da informação ou falha de proteção, ou situação previamente desconhecida que possa ser relevante em termos de segurança.

Exposição: circunstancia de estar exposto aos prejuízos oriundo de um agente ameaçador.

Gestão de incidente da segurança da informação: processo para identificar, reportar, avaliar, responder, lidar, e aprender com os incidentes de segurança da informação.


Gestão da segurança da informação: dirigir e controlar uma organização no que se refere ao risco.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Definições para a Segurança da Informação



Incidente de Segurança da Informação: um único ou uma série de eventos de segurança da informação, indesejáveis ou inesperado, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameacem a segurança da informação.

Integridade: proteger a exatidão e a integridade dos ativos, prevenir contra modificações não autorizadas, por pessoas não autorizadas ou processos.

Não repúdio: habilidade de provar a ocorrência de suposto evento ou ação e suas entidades de origem.

Política: intenção e orientação geral formalmente expressa pela administração.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Definição de Segurança da Informação

Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

(ABNT NBR ISO/IEC 27002: 2005)

Quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente.

Lyra, 2008



Auditoria e Segurança da Informação

Pilares da Segurança da Informação

Confidencialidade: “Garantia de que o acesso à informação é restrito aos seus usuários legítimos.” Ou seja, seu acesso é permitido apenas a determinados usuários.

Integridade: “Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais”. Ou seja, informação não adulterada.

Disponibilidade: “Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna”. Ou seja, independente da finalidade, a informação deve estar disponível.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Garantia da Segurança da Informação

Autenticação: “Garantir que um usuário é de fato quem alega ser”.

Não repúdio: “Capacidade do sistema de provar que um usuário executou uma determinada ação”.

Legalidade: “Garantir que o sistema esteja aderente à legislação”.

Privacidade: “Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações”.

Auditoria: “Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque”.



Auditoria e Segurança da Informação

Conceitos para a Segurança da Informação

O que estamos protegendo.

Do que estamos protegendo.

Análise de Risco.



Requisitos de segurança são identificados através de análise de riscos.

O resultado da análise dos riscos ajudarão a guiar e a determinar a ação apropriada de gestão e as prioridades para gerenciar os riscos de segurança da informação.

A análise de risco deve ser repetida periodicamente para tratar das mudanças que podem influenciar os resultados da avaliação de risco.

Auditoria e Segurança da Informação

Conceitos para a Segurança da Informação

A Segurança da Informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, implementados, monitorados, revisados e melhorados, para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos



Auditoria e Segurança da Informação

Conceitos para a Segurança da Informação

A abordagem de processo para a Segurança da Informação apresentada na ISO 27002:2013 “Código de prática para a segurança da informação” (*Code of practice for information security*).

- ✓ Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para segurança da informação.
- ✓ Implementar e operar controles para gerenciar os riscos da segurança da informação da organização no contexto dos riscos gerais da organização.
- ✓ Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (*Information Security management System – ISMS*).
- ✓ Melhoria continua baseada em medições objetivas



Auditoria e Segurança da Informação

Conceitos para a Segurança da Informação

Definir, alcançar, manter e melhorar a segurança da informação pode ser essencial para manter a vantagem competitiva e observância da lei.

As empresas e seus sistemas de informação e redes enfrentam ameaças de segurança provenientes de várias fontes.



- ❖ Fraudes assistidas por computador
- ❖ Espionagem
- ❖ Sabotagem
- ❖ Vandalismo
- ❖ Incêndio ou inundação

Auditoria e Segurança da Informação

Conceitos para a Segurança da Informação

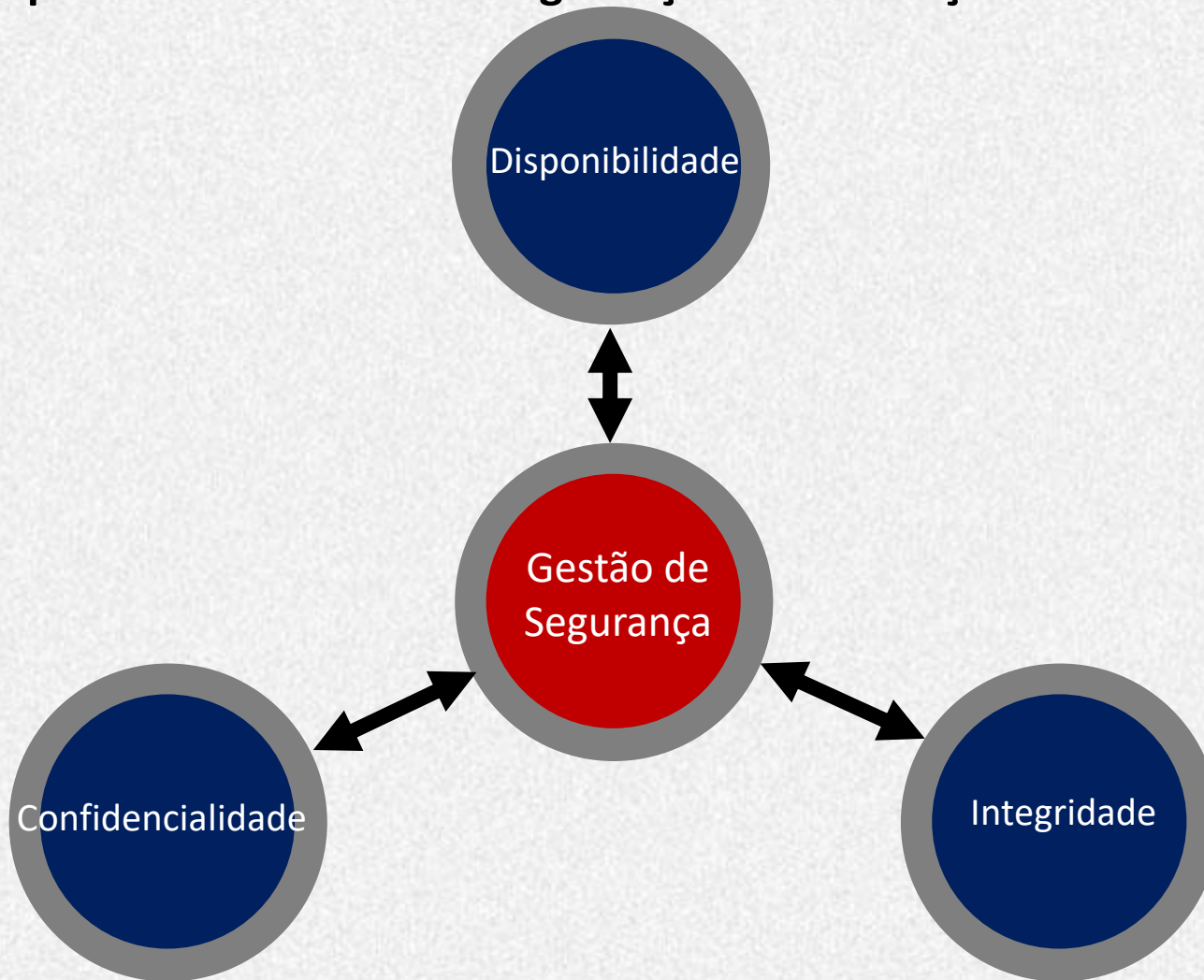
- ❖ Códigos maliciosos
- ❖ Atividades de *hacking*
- ❖ Atividades de negação de serviço (*denial-of-service*)



Tornaram-se mais comuns, mais ambiciosos e cada vez mais sofisticados

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação



Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Confidencialidade



Também chamada exclusividade.

É referente à quem pode ter acesso ao tipo de informação.

Os executivos podem ter a preocupação de proteger seus planos estratégicos em relação aos concorrentes.

As pessoas estão preocupadas com o acesso aos seus dados financeiros.

Assegura que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada .

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Confidencialidade

A confidencialidade pode ser oferecida através de **criptografia dos dados** à medida que são armazenados e transmitidos.

Pode ser utilizada:

- ✓ Preenchimento de Tráfego na rede (*Traffic padding*),
- ✓ Estrito controle de acesso.
- ✓ classificação dos dados.
- ✓ Treinamento de pessoal.



Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Confidencialidade

- ✓ Acesso à informação é concedida com base na “necessidade de conhecer”.

Um funcionário do Financeiro não tem necessidade de ver relatórios de discussão com clientes.

- ✓ Funcionários tomam medidas para garantir que a informação não vá para pessoas que não necessitem dela.

Funcionários asseguram que nenhum documento confidencial seja deixado sobre suas mesas enquanto estão ausentes.

- ✓ O gerenciamento de acesso lógico assegura que pessoas e processos não autorizados não tenham acesso a sistemas não autorizados.

O usuário não tem o direito de alterar as configurações do PC.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Confidencialidade



- ✓ Criar uma separação de funções entre a organização de desenvolvimento de sistemas, a organização de processamento e a organização do usuário.

O desenvolvedor não pode alterar salários.

- ✓ São criadas separações estritas entre o ambiente de desenvolvimento, o ambiente de teste, aceitação e produção.

No processamento e uso dos dados, são tomadas medidas para garantir a privacidade do pessoal e de terceiros.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Integridade



É referente a ser correto e consistente com o estado da informação pretendida.

Alteração de dados acidental ou não é considerado violação na integridade dos dados.

Os dados armazenados em disco devem ser estáveis, não podem ser alterados aleatoriamente por problemas.

Os programas de aplicações não devem gravar informações incorretas e valores diferentes dos esperados.

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Integridade

“Integridade significa que a informação é completa, perfeita e intacta (não necessariamente correta). Significa que nada está faltando na informação, ela está completa e em um bom estado “

Donn Parker, apud Hintzbergen, 2015, p. 30

A informação pode ser incorreta ou não autêntica, mas possuir integridade, ou ser correta e autêntica, mas não possuir integridade.

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Integridade

O ambiente deve assegurar que atacantes, ou erros de usuários, não comprometam a integridade dos sistemas de dados.

Quando um atacante insere um vírus, uma bomba lógica ou um *backdoor* em um sistema, a integridade é comprometida.



Essa invasão é denominada, **corrupção**, **invasão maliciosa** ou **substituição de dados por dados incorretos**.

Essa ação deve ser combatida por **Controle de Acesso**, **Detecção de intrusão** e **Hashing**.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Integridade

Usuários normalmente afetam o sistema ou a integridade do sistema por erro.
Mas também podem cometer atos maliciosos.

Usuários normalmente afetam o sistema ou a integridade do sistema por erro.
Mas também podem cometer atos maliciosos.

Os usuários podem involuntariamente apagar arquivos de configuração supondo equivocadamente que não haveria problema.



EDUCAÇÃO
METODISTA

Auditoria e Segurança da Informação

Princípios Fundamentais da Segurança da Informação - Integridade

Medidas de integridade

Mudanças em sistemas e dados autorizados: Um membro da equipe atribui um novo preço a um artigo no *website* e outro verifica a validade desse preço antes de ser publicado.

Mecanismos para pessoas utilizarem o termo correto: Um cliente é sempre chamado de “cliente”, não pode ser inserido outro termo como “freguês”.

Gravação das ações de usuários (log): identificar quem modificou a informação.

Ações vitais para o sistema: As instalações de softwares novos não podem ser conduzidas por uma pessoa somente. Ao segregar funções, posições e autoridades, pelo menos duas pessoas são necessárias.



Auditoria e Segurança da Informação



Atividade 1

Realizar a **leitura individual** do artigo:

O que o futuro pós-pandemia reserva para os auditores de TI

Disponível em:

<https://www.isaca.org/resources/news-and-trends/industry-news/2023/what-the-post-pandemic-future-holds-for-it-auditors>

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

1. Para atender as exigências de clientes exigentes, requer sistemas mais sofisticados, Como os auditores de TI podem ajudar as organizações a conseguirem a utilização dessas tecnologias?
2. O autor, como exemplo, relata o caso da empresa francesa Kering. Quais os cenários que o CEO François-Henri Pinault, explicou que podem ser testados?
3. Como o cliente pode utilizar a Realidade Aumentada e Realidade Virtual? Cite exemplos que não foram citados no artigo.
4. O que os Auditores de TI devem fazer para minimizar os fatores de riscos quando os investimentos em TI não atingem seus objetivos iniciais?
5. O autor cita que as abordagens tradicionais de auditoria estão obsoletas, O que os auditores devem fazer para realizar a auditoria?
6. Quais os desafios que as novas tecnologias colocam?

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