AUDITORIA DE SISTEMAS

UNIDADE 2 – GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Autor:
Wellington Ávila
Revisor:
Jaime Gross Garcia

Introdução

Caro(a) estudante,

No mundo atual, com inúmeras transformações do mercado e inovações tecnológicas que contribuem para a competitividade, as organizações passam a adotar sistemas integrados de gestão, que impulsionam outros sistemas de apoio aos negócios, como os sistemas administrativos, de relacionamento com os clientes e de produção e logística.

Portanto, quando falamos em sistemas computacionais de apoio aos negócios, não é possível deixar para segundo plano o tratamento das informações que circulam nesses sistemas, pois todos os dados e informações pertinentes ao bom funcionamento do negócio estão se relacionando nessas plataformas. Nesta unidade, vamos conhecer a gestão estratégica e a análise de riscos, bem como os tipos de ameaças, os riscos e vulnerabilidades dos sistemas de informação (SI), as normas e procedimentos, assim como os riscos que envolvem as informações.

Bons estudos!

2.1 Gestão estratégica e análise de riscos

Os sistemas precisam gerar informações confiáveis, visando dar suporte à tomada de decisão no nível estratégico de qualquer organização, seja ela no âmbito público ou privado. Para que as informações proporcionem eficiência e valor aos negócios, a gestão estratégica e a análise de riscos precisam participar como parte do processo, visando garantir sua qualidade. Para tal, a estrutura do processo deve possuir os princípios básicos da segurança da

informação, como: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

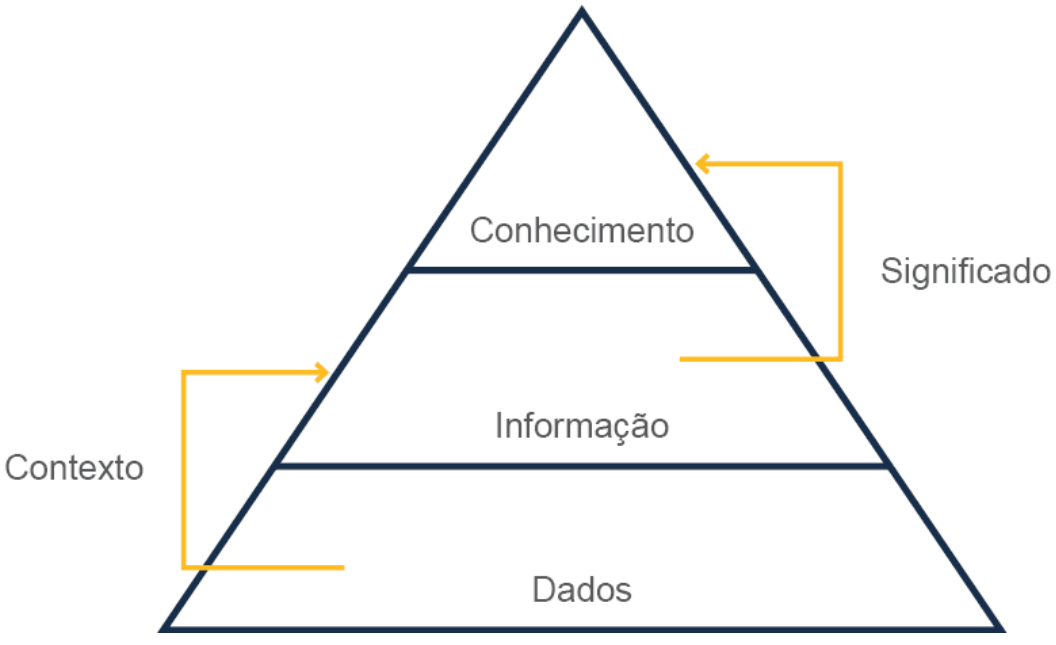
Hierarquia de sistemas de informação

NÍVEL	CARACTERÍSTICAS
SIs em nível operacional	São utilizados em situações cotidianas. São previsíveis e de efeito imediato. Ocorrem, normalmente, quando um gerente de produção necessita substituir um equipamento por falhas, por exemplo.
SIs em nível gerencial	São utilizados quando as informações requerem um tratamento detalhado, de forma mais analítica, proveniente de diversas fontes. Proporcionam efeitos mais amplos, como o lançamento de uma campanha de marketing de um produto ou serviço. São casos que contemplam a transformação das informações agrupadas para a gestão.
SIs em nível estratégico	Quando as situações são mais complexas, geralmente de difícil solução. São decisões que envolvem a mais alta incerteza, como a inserção de uma empresa em um novo mercado ou mesmo a fusão entre empresas.

Fonte: KOLBE, 2017, p. 53. (Adaptado).

Para que a tomada de decisão seja assertiva por parte de um corpo executivo, é necessário que se analise a confiabilidade dos dados. Nesse sentido, podemos dizer que as informações são dados contextualizados e que o conhecimento, por sua vez, é construído por informações que, em um determinado momento, ganharam um significado específico. É a partir da existência desse conhecimento que se torna possível tomar decisões. Nesse sentido, é importante compreender que o conhecimento só pode ser construído a partir da informação, que é a matéria-prima do conhecimento.

Infográfico 1 - Pirâmide do conhecimento



Fonte: KOLBE, 2017, p. 53. (Adaptado).

#PraCegoVer: Na figura, representada por uma pirâmide, dividida em três níveis, é possível compreender, de baixo para cima, o primeiro nível chamado Dados, em letras maiúsculas. A seguir, há o segundo nível denominado Informação, e no topo da pirâmide, o terceiro nível, denominado conhecimento. A imagem possui, ao lado esquerdo, uma seta amarela, que aponta, de Dados, até o nível de informação, indicando que a informação se constitui de dados contextualizados. Ao lado direito, no nível Informação, há uma seta apontando para o nível acima, indicando que o conhecimento é construído a partir das informações e seus respectivos significados.

Os dados, as informações e o conhecimento são praticamente a base de um processo de tomada de decisões, um dá suporte ao outro na formação da sabedoria. Devido os dados serem a base de toda a construção até a sabedoria, mostra-se exatamente a importância da proteção deles junto às informações. A gestão estratégica e a análise de riscos presentes diariamente nos processos de negócios asseguram a proteção dos dados e das informações inseridas em algum sistema computacional garantindo a segurança necessária.

Informação não é um termo exclusivamente matemático. É, também, um termo filosófico por estar ligado à qualidade da realidade material a ser organizada, criada ou classificada em um sistema. Para Manoel (2014):

> **Informação é o resultado do processamento de dados, gerando algum tipo de conhecimento. Essa informação só é importante ou valiosa se fizer a diferença para quem manipula. A informação pode ser constituída por um conjunto de dados que representam um ponto de vista diferente, revelando um significado novo ou trazendo elementos antes desconhecidos para quem manipula. Ela causa impacto em grau maior ou menor, sendo elemento essencial da criação de conhecimento para determinado assunto (MANOEL, 2014, p. 18).**

Diante do mencionado, é possível entendermos a importância da existência e emprego da segurança estratégica junto à análise de riscos nas empresas. Assim, no contexto da informação, a gestão estratégica ganhou o "papel de protagonista" nas organizações, sendo em grande parte a responsável pelo destaque positivo no mercado e o sucesso nos negócios.

As organizações que buscam se destacar no mercado competitivo estão constantemente buscando utilizar suas informações de maneira estratégica. Para tal, as informações precisam estar disponíveis e gerenciadas por meio da gestão estratégica da informação.

É importante as organizações entenderem, nesse mundo altamente tecnológico, que é impossível ignorarem os efeitos causados pela era das evoluções e inovações digitais. Como os recursos humanos no passado eram exclusivos nas organizações, hoje ele ganha mais um aliado com grande perfil de importância para a sobrevivência corporativa, que é a informação. As empresas se tornaram dependentes da informação, já que essa é vital para a tomada de decisões corporativas.

Durante um grande período, a segurança da informação era tratada nas organizações como um assunto de responsabilidade exclusiva dos profissionais de informática, pois não havia envolvimento próximo com a alta gestão. Atualmente, a segurança da informação é vista de forma diferente nas organizações. Assim, ela possui mais que uma tradicional estrutura hierárquica em recursos humanos e tecnologias, e como requer o envolvimento de gestores em procedimentos exclusivos que demandam um perfil gerencial, ela exige um ambiente seguro para que possa garantir uma proteção eficaz dos dados e processos que os utilizam.

Com a gestão envolvida, referente às necessidades e exigências emergenciais da segurança da informação, é

possível mensurar também os valores dos investimentos financeiros, visando evitar prejuízos e viabilizar transações.

É preocupante que mesmo com a existência e a adoção de inúmeros procedimentos de proteção, medidas de conscientização organizacional, instalação de tecnologias, entre outras, ainda seja necessário o constante monitoramento, controle e alerta das informações referentes ao crescimento incessante de incidentes de segurança da informação. Inevitavelmente, as organizações, de diversos portes e tipos de negócios, estão mais expostas às formas de ataques inovadoras emergentes, inclusive no Brasil.

Com os altos custos para manter os seus ativos de informação protegidos de ameaças, as organizações precisam trabalhar com a gestão estratégica, alinhada à análise de riscos, visando garantir que processos e sistemas dependentes de toda a estrutura de informações estejam com os seus riscos minimizados às novas ameaças.

A gestão da segurança estratégica possui ferramentas e técnicas que contribuem para a proteção das informações: elas estão classificadas em três camadas: física, lógica e humana. Cada camada possui sua respectiva função, ação, critério e significado, visando o estabelecimento de segurança para as informações.

» Camada física

Trata-se do ambiente utilizado para acessar às informações corporativas, localizado e instalado fisicamente no hardware, seja em ambiente corporativo ou residencial, como o trabalho remoto ou de home office. A camada física é o ambiente em que estão localizados os computadores, servidores, meios de comunicação e seus demais periféricos, inclusive as redes de computadores e seus equipamentos, como os modems.

Algumas organizações possuem seus dados e informações armazenadas em servidores e em estações compartilhadas, o que é preocupante, já que em alguns casos não há restrições em relação ao acesso físico desses equipamentos. Muitas vezes, é possível encontrar computadores que possuem acesso liberado à internet, livre para qualquer usuário. Assim, os computadores que se encontram na condição mencionada estão vulneráveis aos riscos e às ameaças, podendo ser as raízes de qualquer incidente de segurança.

As organizações que levam a questão dos riscos e ameaças a sério tendem a conscientizar seus colaboradores, treinando os profissionais técnicos de informática em segurança da informação, cada um em suas respectivas esferas de tratamento e conhecimento. Assim, o objetivo da camada física é proteger as informações e equipamentos em relação aos acessos não autorizados, prevenindo, também, danos oriundos de causas naturais. A camada física, contudo, não está somente relacionada ao aspecto informatizado do processo, mas também está interligada aos fatores que envolvem a ação humana. A seguir, algumas das funcionalidades da camada:

- Controlar o acesso de visitantes;
- Prevenir acessos físicos às instalações sem a devida autorização;
- Prevenir contra incêndio;
- Proteger e controlar os servidores em relação ao acesso físico;
- Proteger o acesso à sala dos servidores.

» Camada lógica

É definida, geralmente, pela utilização de softwares e programas que administram as funcionalidades e desempenhos dos hardwares, com a execução de transações automatizadas, criptografia de mensagens e senhas. Assim, os protocolos de comunicação de transações e consultas ficam localizados nessa camada.

As aplicações localizadas nos ambientes informatizados e que os usuários possuem algum tipo de acesso recebem a classificada segurança de nível lógico, independentemente do tamanho ou da capacidade do computador ou do tipo de aplicação que será executada. Os controles e ferramentas utilizadas são “transparentes” para os usuários e passam despercebidas, somente sendo notadas no momento de algum bloqueio ao acesso realizado pelo controle de acesso.

Uma medida simples e importante é manter as configurações do sistema operacional de acordo com a versão do fabricante, sempre procurando atender às recomendações de atualização mais recente do sistema e suas correções voltadas para segurança. A presente medida ajuda na minimização de riscos de segurança na camada lógica.

Nesse sentido, o objetivo dessa camada é a aplicação de medidas e procedimentos que visam proteger os dados, sistemas, programas, arquivos ou qualquer recurso de rede contra as tentativas de acesso sem autorização por usuários, processos de rede ou programas maliciosos.

VOCÊ QUER LER?

Encontre mais informações sobre algumas medidas que podem reforçar a segurança dos sistemas:

• Atualizar e instalar o sistema de firewall pessoal e de antivírus;
• Atualizar por patches os aplicativos com suas devidas correções, de acordo com as recomendações do fabricante;
• Controlar as informações de entrada e saída utilizando um filtro pelo firewall;
• Detectar e vetar a instalação de programas suspeitos no computador;
• Detectar, pelo sistema, a intrusão nos programas e sistemas;
• Realizar o backup e redundância dos dados dos sistemas e aplicativos;Registrar informações pertinentes ao evento executado.

» Camada humana

Trata-se da camada mais crítica da empresa e que demanda a maior atenção; já que é formada por todos os colaboradores da organização, em especial os profissionais que trabalham na manutenção dos recursos tecnológicos e que possuem algum tipo de acesso aos sistemas. A presente camada, conforme o próprio nome, aproxima-se dos aspectos comportamentais das pessoas, inclusive dos que podem ter alguma ligação com a origem dos riscos pela ação humana.

Por lidar com a questão humana, essa camada torna-se complexa para avaliação dos riscos, bem como para o gerenciamento da segurança, porque o fator humano é considerado, para a segurança da informação, como o "elo mais fraco da corrente". Isso se dá devido às características individuais dos indivíduos, como as psicológicas, emocionais ou sociais, por exemplo, que variam de pessoa para pessoa.

Logo, para que qualquer organização atenda aos requisitos mínimos de segurança, a gestão da segurança da informação deve atender satisfatoriamente aos controles eficientes em todas as camadas.

> **A gestão da Segurança da Informação tem por objetivo o planejamento, a execução e a monitoração das atividades de SI, e a aplicação de processos e melhoria contínua. Sem isso, a GSI ficaria somente no mundo das ideias e não traria nenhum resultado positivo e significativo para a organização (MANOEL, 2014, p. 65).**

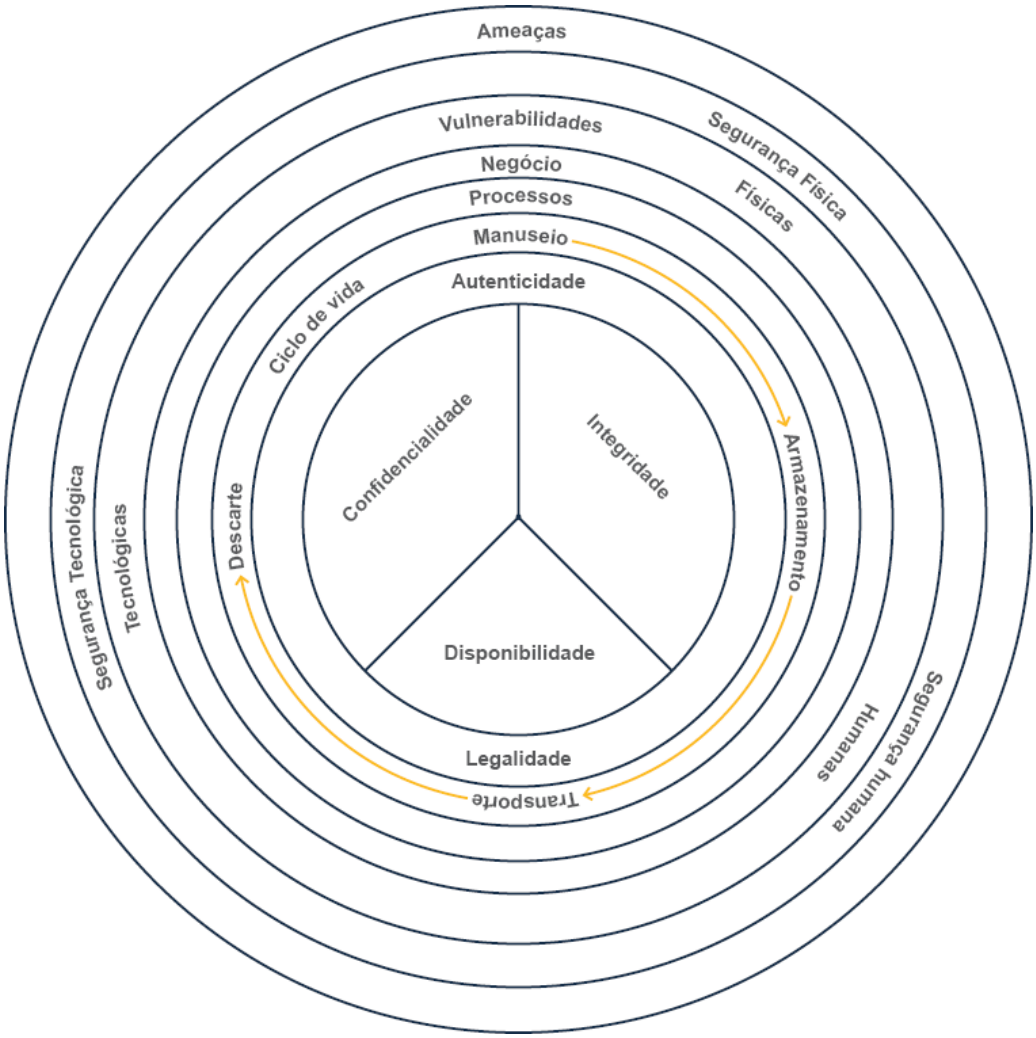
As camadas citadas possuem características particulares de acordo com a sua respectiva funcionalidade, visando o alcance e o respectivo tratamento às diferentes partes da segurança da informação.

A camada humana serve como referência e orientação para os processos seletivos e contratações. Para tal, deve ser previamente informada a existência de uma política de segurança a ser seguida e cumprida pelo usuário e que, havendo o seu descumprimento, ele estará sujeito a penalidades, de acordo com a modalidade da infração cometida.

Em uma organização, podem existir funcionários de áreas diferentes da tecnologia da informação, conhecedores de técnicas e ferramentas que permitem a invasão de sistemas, violação de senhas, dados e informações.

O Infográfico a seguir retrata um possível impacto gerado por um incidente de segurança. Por meio dele, é possível analisar a dimensão em que os desafios estão distribuídos na área de segurança da informação nos mais diversos ambientes organizacionais.

Infográfico 2 - Descrição dos ataques sintáticos e ataques Semânticos



Fonte: SÊMOLA, 2014, p. 49. (Adaptado).

#PraCegoVer: na figura em círculo é possível compreender os desafios em forma de camadas, sendo dividida em oito. De dentro para fora no centro do círculo está a informação dividida em seus pilares, como a confidencialidade, integridade e disponibilidade. Na próxima camada estão os outros princípios que norteiam a segurança da informação, como a autenticidade e a legalidade. Na próxima camada é encontrado o ciclo de vida da informação, como o manuseio, armazenamento, transporte e o descarte. Na camada seguinte, é possível identificar os processos e ativos. A próxima camada é representada pelo negócio. Em seguida aparecem dividindo a próxima camada as vulnerabilidades tecnológicas, físicas e humanas.

No nível seguinte é possível identificar, dividindo a próxima camada, a segurança tecnológica, segurança física e segurança humana. Por fim envolvendo todo conteúdo mencionado, a camada chamada de ameaças.

Recomenda-se que as camadas de segurança da informação sejam aplicadas na gestão da segurança da informação, visando a proteção de sistemas informatizados identificados com alta criticidade em relação às vulnerabilidades e ataques de criminosos virtuais.

VAMOS PRATICAR

Experimente listar brevemente algumas qualificações que um profissional de gestão de segurança da informação precisa ter para o sucesso em sua atuação diante de suas responsabilidades e atribuições. Para ajudar nessa elaboração, leia o artigo "Segurança da informação: conheça as 12 melhores práticas", no site Panorama Positivo de Olho na Tecnologia. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao>.

2.2 Tipos de ameaças, riscos e vulnerabilidades dos sistemas de informação

Constantemente a internet está sendo utilizada para diversas finalidades, desde a compra e venda de produtos e serviços, educação na modalidade à distância, relacionamentos através das redes sociais, até serviços financeiros. Assim, é possível afirmar que a internet já faz parte da vida das pessoas. Em contrapartida, aproveitando-se da grande utilização do uso constante dos serviços online pelos usuários, estão os criminosos virtuais, prontos para aplicarem seus golpes, sequestro de dados e executar códigos maliciosos.

A técnica de engenharia social é a mais utilizada na viabilidade dos crimes, pois os criminosos trabalham com o anonimato virtual, visando minimizar os riscos e maximizar os lucros ilícitos. Assim, as práticas criminosas compensam mais no meio cibernético do que no mundo real. Logo, diante de uma certa facilidade, grande parte dos crimes que eram cometidos fisicamente migraram para a rede. O que facilita a ação dos golpistas virtuais é a ausência de uma lei de crimes cibernéticos exclusiva, a falta de conhecimento em segurança da informação por parte das pessoas e a ausência de uma política severa pertinente aos crimes na modalidade digital.

As organizações que desejam estar com suas informações protegidas precisam, no mínimo, conhecer os processos internos, métodos e tecnologias que usam, inclusive a prospecção de evolução no que se refere à adoção de novos sistemas ou a implementação de tecnologias inovadoras. Dessa forma, através de um breve planejamento, é possível identificar, com mais facilidade, os possíveis ataques, bem como o perfil dos atacantes, buscando métodos emergenciais de defesa.

As ameaças são variadas em relação aos sistemas informatizados, pois podem deixar boa parte do sistema inoperante ou então violar os dados e as informações da plataforma. Contudo, reconhecendo o tipo de ameaça aos sistemas, é possível identificar e mensurar os riscos, avaliando a probabilidade e o impacto dos ataques. Logo, as formas de prevenção precisam ser oportunas e proativas. Para tal, é preciso haver coerência nos métodos organizados e utilizados na proteção das informações nos sistemas.

A seguir, exemplos de ameaças consideradas da nova geração:

ARMAZENAMENTO DE SENHAS EM FORMATOS RECUPERÁVEIS	A vulnerabilidade armazena senhas e logins em formatos que proporcionam sua recuperação, viabilizando ações ilícitas que utilizarão esses dados. A ação criminosa pode ser realizada por meio do acesso ao sistema como administrador, que com as permissões corretas, pode recuperar as senhas e os respectivos logins, o que viabiliza invasões de contas;
BUFFER OVERFLOW (ESTOURO DE BUFFER OU TRANSBORDAMENTO DE DADOS)	Trata-se da forma mais conhecida de vulnerabilidade. Ocorre quando o sistema excede o limite de uso de memória atribuído a ele pelo sistema operacional, e logo após os dados são inseridos na parte externa aos limites da adequação de memória, ficando ela subscrita pelos caracteres extras, ocasionando o corrompimento de dados, que pode gerar erros ou até mesmo a execução de códigos maliciosos;
COMPOSITE THREATS (AMEAÇAS COMPOSTAS)	São ataques classificados como compostos ou combinados. Eles são uma junção dos ataques sintáticos e semânticos, classificação dos ataques cibernéticos que está detalhada nas Abas a seguir.

Descrição dos ataques sintáticos e ataques semânticos

ATAQUES	DESCRIÇÃO
Ataques sintáticos	São ataques diretos considerados como um software malicioso, incluindo vírus, *worms* e cavalo de tróia.
Ataques semânticos	São ataques capazes de realizar a modificação e a disseminação de informações corretas e incorretas, com ou sem o uso da tecnologia.

Os riscos diante das diversas ameaças são um desafio para as equipes de segurança da informação, pois elas precisam entender o atual contexto das ameaças, bem como identificar importantes pontos de ameaça e seus atores, seus alvos específicos, os focos de intenção do ataque arquitetado, métodos, táticas, técnicas e procedimentos.

Os sistemas de informação podem ser considerados parcialmente como livres de ataques, mas as vulnerabilidades fazem parte de todos os sistemas informatizados, gerando preocupação constante para os profissionais atuantes em suas respectivas ações e técnicas de segurança. Dessa forma, elas precisam receber atenção e o tratamento adequado para não evoluírem.

Nesse sentido, a vulnerabilidade dos sistemas de informação pode ser compreendida como uma fragilidade da aplicação, gerada por diversos motivos, como o descuido em seu desenvolvimento ou indevida implementação de proteção ou bug sistêmico.

- **Cross Site Scripting (XSS)**: trata-se de uma vulnerabilidade mais comum, que possui a capacidade de atingir os servidores de ambientes, aplicativos e web. Essa vulnerabilidade aceita ataques por injeção, devido a não validação criteriosa, permitindo a execução de scripts de terceiros. Conforme as páginas e os aplicativos recebem acessos, são executados códigos arbitrários, por haver um portal de entrada e saída localizado em

uma zona privilegiada propícia à ocorrência;

- **Polymorphic threats (ameaças polimórficas)**: são ameaças caracterizadas como ataques cibernéticos, como vírus, *worm* ou cavalo de tróia, que possuem a capacidade de mudar constantemente. As ameaças polimórficas podem realizar maliciosamente, por exemplo, a alteração do nome de arquivos e sua compactação. As ameaças polimórficas apresentam uma aparência variável referente ao código, e elas realizam mutações, cuja função objetiva se mantêm como a original;
- **Portabilidade**: trata-se de implementações realizadas de forma inconsistente entre as versões de sistemas operacionais ou entre os próprios, podendo ser potenciais fontes de vulnerabilidades. Devido aos aplicativos na nuvem serem usados por vários dispositivos e por diferentes versões de sistemas operacionais, eles acabam sofrendo problemas de vulnerabilidade;
- **Vazamento de informação**: a vulnerabilidade ocorre quando há a revelação de informações inseridas no sistema. Isso pode facilitar uma ação criminosa, devido ao conhecimento que o atacante possuirá para arquitetar sua atividade ilícita. Tecnicamente, é considerado que a informação saia da aplicação por meio da interceptação de logs;

Teste seus conhecimentos

ATAQUES SINTÁTICOS E SEM NTICOS

No mundo da segurança da informação existem duas classificações específicas para os ataques, sendo eles, os ataques sintáticos e os ataques semânticos, que, combinados, são a origem das conhecidas ameaças compostas ou em inglês composite threats. Considerando essas informações, analise as asserções a seguir e a relação proposta entre elas.

I. Os ataques são divididos em semânticos e sintáticos, sendo que estes últimos são diretos e considerados como um software malicioso, incluindo vírus, worms e cavalo de Tróia.
Porque:
II. Os ataques semânticos são capazes de realizar a modificação e a disseminação de informações corretas e incorretas, com ou sem o uso da tecnologia.

A seguir, assinale a alternativa correta:

a As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I.

b As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.

c A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

d A asserção I é uma proposição falsa, e a II é uma proposição verdadeira.

e As asserções I e II são proposições falsas.

Gabarito na página 23.
Atividade não pontuada.

2.3 Elementos e normas

As redes sociais possuem determinados grupos de pessoas com diferentes opiniões, culturas, crenças, valores, entre outras características pessoais, que variam de membro para membro-usuário em uma rede. Contudo, mesmo com a liberdade que cada usuário possui para escolher, são estabelecidos pelos próprios grupos e pelas redes sociais normas e padrões que deverão ser seguidos, para que os usuários possam ser aceitos, permanecendo como membros.

No caso mencionado, as normas permitem o estabelecimento de critérios mínimos que servirão como um guia para a aceitabilidade e julgamento das relações sociais de um membro do grupo ou de todos os outros. Logo, as normas possuem como objetivo a harmonia das melhores práticas, de maneira que sejam seguidas as mesmas orientações e perspectivas sobre um determinado tema.

Diagrama 1 – Objetivos da normalização

Fonte: ABNT, 2006. (Adaptado).

#PraCegoVer: Na figura são apresentados os objetivos da normalização, sendo um círculo maior localizado no centro e a sua volta os oito objetivos representados em círculos menores, como: segurança, proteção do produto, controle da variedade, proteção do meio ambiente, intercambialidade, eliminação de barreiras técnicas e comerciais, compatibilidade e comunicação.

Além disso, as normas podem ser consideradas um conjunto de diretrizes, padrões e regras aplicáveis, cujo objetivo é orientar comportamentos ou especificações técnicas, entre outros critérios, dependendo do contexto de sua aplicação. Por exemplo, é possível considerar o Código Civil e o Código de Defesa do Consumidor como normas. De acordo com a ABNT (2006):

> **O objetivo da normalização é o estabelecimento de soluções, por consenso das partes interessadas, para assuntos que têm caráter repetitivo, tornando-se uma ferramenta poderosa na autodisciplina dos agentes ativos dos mercados, ao simplificar os assuntos, e evidenciando ao legislador se é necessária regulamentação específica em matérias não cobertas por normas.**
>
> **Qualquer norma é considerada uma referência idônea do mercado a que se destina, sendo por isso usada em processos: de regulamentação, de acreditação, de certificação, de**

metrologia, de informação técnica, e nas relações comerciais Cliente - Fornecedor. (ABNT, 2006)

As normas são importantes aliadas em uma gestão de segurança da informação (GSI), por exemplo, partindo do princípio que o fator humano é crítico e ao mesmo tempo delicado. Nesse sentido, as normas serão um direcionamento que ajudará na análise e controle do comportamento humano.

Características básicas das normas para gestão da segurança da informação

NORMAS	CARACTERÍSTICAS
ISO/IEC 27000: 2018	**Data de publicação**: 7-fev-18 **Título**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Visão geral e vocabulário. **Objetivo**: Explicar a série de normas, objetivos e vocabulários.
ISO/IEC 27001: 2013	**Data de publicação**: 8-nov-13 **Título**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos **Objetivo**: Especificar os requerimentos, visando estabelecer, implementar, monitorar e rever, mantendo e provisionando um sistema de gerenciamento completo. É utilizado o ciclo PDCA como fundamento da norma, sendo ela certificável para as organizações.
ISO/IEC 27002: 2017	**Data de publicação**: 8-nov-13 **Título:** Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação **Objetivo**: apresentar o caminho de como alcançar os controles certificáveis pertinentes à ISO 27001. É certificável para profissionais, mas não para as organizações.
ISO/IEC 27003: 2017	**Data de publicação**: 24-abr-20 **Título**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Orientações **Objetivo**: fornece diretrizes práticas para a implementação de um sistema de gestão da segurança da informação em uma organização, conforme a ABNT NBR ISO/IEC 27001:2005.
ISO/IEC 27004: 2016	**Data de publicação**: 29-ago-17 **Título**: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Monitoramento, medição, análise e avaliação. **Objetivo**: apresentar como mensurar a eficácia do sistema de gestão de segurança da informação em uma organização.

ISO/IEC 27005: 2019	**Data de publicação**: 24-out-19 **Título**: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação **Objetivo**: controlar todo ciclo de controle de riscos da organização e atuar juntamente à ISO 27001 nos casos de certificação, ou por meio da ISO 27002 em situações de somente implantação.
ISO/IEC 27006: 2015	**Data de publicação**: 30-set-15 **Título**: Tecnologia da informação - Técnicas de segurança - Requisitos para organismos que fornecem auditoria e certificação de sistemas de gestão de segurança da informação **Objetivo**: especificar como deve ocorrer o processo de auditoria de um sistema de gerenciamento de segurança da informação.
ISO/IEC 27007: 2020	**Data de publicação**: 21-jan-20 **Título**: Segurança da informação, cibersegurança e proteção da privacidade - Diretrizes para auditoria de sistemas de gerenciamento de segurança da informação **Objetivo**: fornecer diretrizes para a gestão de um programa de auditoria do sistema de gestão de segurança da informação e para a realização de auditorias por parte das competências dos auditores. É um documento cuja aplicação busca o conhecimento e a realização de auditorias internas ou externas no gerenciamento do programa de auditoria mencionado.
ISO/IEC 27008: 2019	**Data de publicação**: 14-jan-19 **Título**: Tecnologia da informação - Técnicas de segurança - Diretrizes para avaliação dos controles de segurança da informação **Objetivo**: fornecer orientações pertinentes à revisão e avaliação da implementação e operação dos controles de segurança da informação, tendo incluído a avaliação técnica dos controles do sistema de informações. Possui como foco o controle, buscando viabilizar a implementação da ISO 27001.
ISO/IEC 27010: 2015	**Data de publicação**: 10-nov-15 **Título**: Tecnologia da informação - Técnicas de segurança - Gestão de segurança da informação para comunicações intersetorial e intersecional **Objetivo**: fornecer diretrizes para contribuir nas melhores formas de comunicar, acompanhar, monitorar grandes incidentes, viabilizando a execução das diretrizes de maneira compartilhada e transparente entre as organizações.

ISO/IEC 27011: 2016	**Data de publicação**: 23-nov-16 **Título**: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base na ISO / IEC 27002 para organizações de telecomunicações **Objetivo**: definir diretrizes que possam suportar a implementação de controles de segurança da informação em organizações do ramo de telecomunicações. O objetivo é instruir as organizações de telecomunicações, para que elas atendam aos requisitos de gerenciamento de segurança da informação, com base em confidencialidade, integridade e disponibilidade. A recomendação é que seja realizada uma implementação com base nos controles e indicações da ISO/IEC 27002.

As normas favoráveis ao desenvolvimento de uma gestão de qualidade, com retorno de resultados mais assertivos, ajudam no estabelecimento de regras, padrões e controles que viabilizam a uniformidade dos processos, tanto relacionados aos produtos, quanto aos serviços. Ademais, há as seções da norma que podem ser divididas por camada.

Quadro 1 – Seções da Norma ISO/IEC 27002 por camada

CAMADA	SEÇÃO	OBJETIVOS
FÍSICA	Gestão das Operações e comunicações	Garantir a operação segura e correta dos recursos de processamento da informação.
	Segurança física e do ambiente	Prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização; impedir perdas, danos, furtos ou comprometimento de ativos e interrupção das atividades da organização.
	Controle de acesso	Controlar acesso à informação; assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; prevenr o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; prevenir acesso não autorizado aos serviços da rede.
	Gestão de incidentes de segurança da informação	Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.

LÓGICA	Aquisição, desenvolvimento e manutenção de Sistemas de Informação	Garantir que segurança é parte integrante de sistemas de informação; prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos;
		Garantir a segurança de arquivos de sistema; manter a segurança de sistemas aplicativos e da informação. Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
HUMANA	Aquisição, desenvolvimento e manutenção de Sistemas de Informação	Gerenciar a segurança de informação dentro da organização; manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.
	Gestão de Ativos	Alcançar e manter a proteção adequada dos ativos da organização; assegurar que a informação receba um nível adequado de proteção.
	Segurança em recursos humanos	Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos.
	Gestão da continuidade do negócio	Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
	Conformidade	Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
	Política de segurança da informação	Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Fonte: SILVA NETTO; SILVEIRA, 2007. (Adaptado).

2.4 Risco envolvendo informações

As organizações dependem das aplicações, conectividades, dispositivos físicos inteligentes e colaboradores íntegros; mas toda essa dependência acaba proporcionando vulnerabilidades aos seus sistemas, aos meios, recursos e dispositivos utilizados nos negócios. Colaboradores considerados peças-chave, inclusive, possuem acessos às informações de alta criticidade na organização, ou seja, eles viabilizam o bom andamento dos processos de negócios e, também por isso, não podem ser vulneráveis à ataques de qualquer natureza.

A seguir, os principais riscos às informações:

» Roubo de dados

É quando um criminoso rouba dados e informações armazenadas em computadores, servidores, sistemas ou outros dispositivos, visando violar a privacidade e criar diversos transtornos com o foco na obtenção de informações confidenciais. Esse crime é um problema para as organizações, bem como para pessoas físicas. O risco de "roubo de dados" envolvendo uma organização pode ocorrer por meios internos ou externos. Esse fato complica a minimização desses incidentes no âmbito interno organizacional, uma vez que os colaboradores possuem acessos às diversas tecnologias utilizadas pela organização. Hintzbergen (2018) afirma que:

> **As violações de segurança da informação realizadas por todo tipo de pessoa dentro da organização dever ser acompanhadas por um processo disciplinar, que está escrito na política da organização e que é abordado durante o treinamento de conscientização (HINTZBERGEN, 2018, p. 76).**

» Espionagem industrial

Trata-se de uma prática ilegal de investigação, que visa obter vantagem competitiva comercial. Ela é realizada de forma secreta, sem prévia formalização de modo, ignorando todas as condutas éticas que asseguram o bom relacionamento entre as organizações. Seu foco está, geralmente, na obtenção de segredos comerciais, fórmulas de produtos exclusivos, planejamento empresarial, entre outros.

Nesse sentido, é importante observar o tipo de colaborador que está sendo contratado, bem como seus objetivos de carreira com a empresa, pois esse tipo de espionagem pode se dar por conta da insatisfação de um colaborador, por exemplo. Logo, a técnica de engenharia social é muito utilizada pelos espiões industriais, já que ela facilita ações criminosas.

» Phishing

Nas organizações, o *phishing* ocorre no disfarce do criminoso em entidade respeitável no mercado, ou pessoa de reconhecimento renomado, tentando uma forma de se aproximar para a invadir via e-mail ou outros recursos organizacionais de comunicação. O risco classificado como "*phishing*" é o mais conhecido pelos criminosos e mais fácil para obterem resultados, isso pelo simples fato de envolver o fator humano.

» Quebra de senha

Ocorre quando os criminosos realizam um processo de recuperação de senhas transmitidas ou armazenadas como dados. Geralmente, para realizar o procedimento, o criminoso utiliza algumas técnicas, como: adivinhação de senha, trojans, *spyware* e *keyloggers*. A "quebra de senha" tem como objetivo a invasão de sistemas, para que dados armazenados e informações sejam danificadas. Por isso, recomenda-se que sejam criadas senhas fortes, que sejam regularmente alteradas, visando a minimização do risco.

» Ransomware

Pode impactar todo um processo ou uma determinada operação, devido ao bloqueio de acesso às informações do sistema, causando inúmeros prejuízos financeiros. Os ransomware são disseminados por e-mails, contendo anexos maliciosos e fraudulentos, inclusive por aplicativos infectados, dispositivos de armazenamento externo e websites comprometidos.

O foco dessa modalidade está em um valor financeiro a ser disponibilizado para o criminoso, em bitcoins (moeda virtual), em troca da liberação do acesso ou bloqueio realizado por ele. O crime é realizado por meio de ameaça e pagamento de resgate. Importante ressaltar que efetuar o pagamento não é garantia que tudo volte ao normal, já que as mensagens podem ser disparadas por robôs e em massa, o que não permite a identificação da origem do pagamento do resgate.

» Funcionários pouco treinados

Um dos fatores mais importantes nas organizações é a questão do treinamento para seus colaboradores, visto que a falta de treinamento para aperfeiçoar e entender melhor suas atividades e o manuseio dos sistemas contribui para vulnerabilidades e para possíveis incidentes de segurança da informação, inclusive quando se tratar do uso da engenharia social. Logo, uma empresa sem conscientização de segurança da informação pode estar "abrindo suas portas" para um grande problema de ataques aos sistemas.

» Dispositivos pessoais (*BYOD*)

Esse risco que pode envolver informações pela utilização de dispositivos pessoais se refere ao acesso realizado à rede sem o consentimento e a prévia autorização da equipe de segurança da informação, bem como a propagação de arquivos maliciosos que possam viabilizar uma invasão. Algumas organizações, para evitar o problema e minimizarem os riscos, fornecem a alguns colaboradores dispositivos exclusivos para fins corporativos.

» Serviço em nuvem

Os aplicativos fundamentados em nuvem podem ser extremamente perigosos, pois possuem inúmeros riscos envolvendo a segurança das informações, já que podem ser acessados de qualquer lugar, independente do momento. Contudo, tudo dependerá da maneira e do nível de segurança com o qual o usuário conduzirá os procedimentos corporativos na plataforma.

» Dispositivos desatualizados

Os dispositivos de rede, como impressoras, roteadores, servidores, entre outros, utilizam firmwares ou softwares que exigem atualizações ou patches para correção de vulnerabilidades e melhoria de desempenho. Sendo assim, a maioria das recomendações voltadas para segurança recomendam desativar todas as atualizações de patches automáticas; entretanto, não são todas as organizações que identificam manualmente as atualizações, o que facilita a invasão de criminosos.

» Escândalo contábil ocorrido pela ausência da auditoria de sistemas envolvendo a informação

Devido da ausência de mecanismos que pudessem estabelecer uma auditoria de segurança confiável dos sistemas informatizados, a empresa Enron, no primeiro semestre do ano de 2002, foi considerada a "protagonista" de um grande escândalo financeiro no mercado de capitais dos Estados Unidos.

A importância de regras e da formação de comitês responsáveis pelas operações organizacionais exigem, dos profissionais envolvidos, conhecimentos de segurança da informação, que serão aplicados na realização de auditorias de sistemas. Além disso, esses profissionais precisam conhecer as possíveis ameaças provenientes das ações humanas, envolvendo corrupção e riscos cibernéticos, aos quais esses sistemas de informações empresariais estão sujeitos.

A Enron, na época, era a sétima maior empresa dos Estados Unidos, considerada séria e transparente na divulgação de suas informações contábeis, sendo a "gigante" no setor de energia. Por outro lado, seu reconhecimento mundial não a livrou dos riscos e vulnerabilidades envolvendo suas informações e sistemas.

O caso Enron motivou a criação da chamada Lei Sarbanês Oxley, ou somente Lei SOX, uma lei americana criada logo após o ano de 2002. Vergueiro (2002) discorre sobre a Lei SOX:

> **A Lei Sarbanes-Oxley foi promulgada com o objetivo de aumentar a confiança nas informações contábeis que as empresas são obrigadas a divulgar (por exemplo: balanço, demonstrações de resultado etc). Essa meta deve ser atingida com os mecanismos criados para se assegurar precisão das informações. A Lei Sarbanes-Oxley procurou: estabelecer critérios de idoneidade aos responsáveis pela elaboração das informações, evitar conflitos de interesse e criar órgãos para cuidar da divulgação (VERGUEIRO, 2002, p. 306).**

VOCÊ SABIA?

No Brasil, a Enron possuía participações em diversas empresas do setor de energia, como a CEG/CEGRio, Gasoduto Brasil/Bolívia, Usina Termoelétrica de Cuiabá, Eletrobolt, Gaspart e na Elektro (empresa paulista de energia elétrica, que atende cerca de 1,6 milhões de consumidores, fundada em 1 de junho de 1998).

Teste seus conhecimentos

QUALIFICAÇÃO DO PROFISSIONAL DE SEGURANÇA DA INFORMAÇÃO

São muitas as funções da área de segurança da informação e elas são muito dinâmicas, o que exige que os profissionais se atualizem constantemente, para que possam contribuir para a diminuição dos riscos de roubo, perdas e alterações indevidas de informações. Por isso, cada vez mais as empresas demandam não somente formação acadêmica, como também certificações e especializações da área de segurança, além de conhecimento em outras áreas da Tecnologia da Informação.
Fonte: GALVÃO, Michele da Costa. **Fundamentos em segurança da informação**. São Paulo, Pearson, 2015. p.26.

Considerando essas informações, analise as asserções a seguir e a relação estabelecida entre elas:

I. A importância de regras e da formação de comitês responsáveis pelas operações organizacionais exige dos profissionais envolvidos conhecimentos de segurança da informação.
Porque:
II. Esses profissionais precisam conhecer as possíveis ameaças provenientes das ações humanas, envolvendo corrupção e riscos cibernéticos, aos quais esses sistemas de informações empresariais estão sujeitos.

A seguir, assinale a alternativa correta:

a As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I.

b As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.

c A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

d A asserção I é uma proposição falsa, e a II é uma proposição verdadeira.

e As asserções I e II são proposições falsas.

Gabarito na página 24.
Atividade não pontuada.

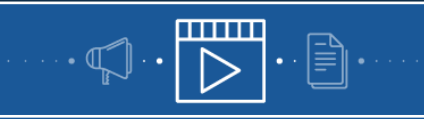
Síntese

Nesta unidade, estudamos a importância dos dados e informações para o mundo, uma vez que são as informações e seus significados que constroem o conhecimento utilizado na tomada de decisões das organizações. Nesse sentido, faz-se importante o conhecimento do papel da gestão da segurança da informação nos diversos negócios que, através da abordagem da gestão estratégica, análise de riscos e a compreensão das camadas da gestão da segurança estratégica, permitem a elaboração de projetos de apoio ao bom andamento dos negócios.

Os sistemas precisam oferecer segurança aos seus dados e informações para não serem fontes de prejuízos aos negócios. Reconhecer os tipos de ameaças, riscos e vulnerabilidade, portanto, foi essencial para serem "traçadas" estratégias de proteção. Além disso, apresentamos os elementos e as normas pertinentes que contribuem para a efetiva gestão da segurança, que visa estabelecer padrões e critérios mínimos de adoção das melhores práticas existentes.

Por último, conhecemos parte do maior escândalo contábil da história mundial, ocorrido pela ausência da auditoria de sistemas envolvendo a informação.

SAIBA MAIS



Vídeo: Modelo de Gestão de Risco em Segurança da Informação: Um estudo de caso no mercado brasileiro de Cartões de Crédito

Autor: Andre Shigueru Hori

Ano: 2003

Comentário: O aumento do fluxo de processos dos negócios, utilizando os sistemas de informação, motivou os criminosos a realizarem suas ações ilícitas explorando as vulnerabilidades e fazendo aumentar os riscos referentes à segurança da informação, envolvendo, de forma específica, a utilização da tecnologia da informação. As pessoas físicas e jurídicas estão inseridas em um cenário que requer cuidados minuciosos com as suas informações, pois a cada ano as ameaças evoluem, desafiando as organizações na adoção de modelos de gestão de riscos em segurança da informação, baseado nas lições aprendidas e as futuras

Onde encontrar?

<http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2216/74539.pdf;jsessionid=3936587ACD8489F5462517F89C9D2DD9?sequence=2>. Acesso em: 09 nov. 2020

Artigo web: Governança de TI: Lei Sarbanes-Oxley (SOX) e a TI

Autor: Emerson Dorow

Ano: 2010

Comentário: A Lei Sarbanes-Oxley foi sancionada visando estabelecer diretrizes e controles necessários, visando a transparência das informações, atendendo os aspectos pertinentes à segurança, veracidade, integridade, entre outros, considerados de criticidade alta em relação às diversas operações que envolvem sistemas e informações existentes nele. As organizações que desejarem ter ações negociadas na Bolsa de Nova York, nos EUA, precisam obrigatoriamente estar em conformidade com a Lei SOX

Onde encontrar?

<https://www.profissionaisti.com.br/governanca-de-ti-lei-sarbanes-oxley-e-a-ti>. Acesso em: 09 nov. 2020

Referências bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **Objetivos**. Disponível em: <http://www.abnt.org.br/normaliz que-e/objetivos>. Acesso em: 25 nov. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **Coletânea Eletrônica de Normas Técnicas - Segura Informação**. Rio de Janeiro, 2020. em: <https://www.abntcatalogo.com.br/pub.aspx?ID=2979>. Acesso em: 25 nov. 2020.

GALVÃO, M. C. **Fundamentos em segurança da informação**. São Paulo, Pearson, 2015. Disponíve <https://plataforma.bvirtual.com.br/Leitor/Publicacao/26525/epub/0? code=U/Nm8DBJJS/3obbEjwI/bttSqVojysx22HSJn+9r5/8sk0opAc6iODmqdem3tJTllL++zu1Ts2mzMRzLyQ37XA==>. Acesso dez. 2020.

HINTZBERGEN, J. et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Rio de Brasport, 2018. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Loader/160044/epub>. Acesso em: 18 nov. 2020.

HORI, A. S. **Modelo de Gestão de Risco em Segurança da Informação: Um estudo de caso no mercado brasileiro de C de Crédito**. São Paulo: Biblioteca Digital FGV, 2020. Disponível <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2216/74539.pdf;jsessionid=3936587ACD8489F5462517F89C9D sequence=2> Acesso em: 09 nov 2020.

KOLBE JÚNIOR, A. **Sistema de Segurança da Informação na Era do Conhecimento**. Paraná, 2017. Disponív <https://plataforma.bvirtual.com.br/Leitor/Publicacao/52012/pdf/0? code=ziBEIX4sJnpGx6oo/FttUCgGVRLAC8DUwKSq/dxQqpTlKzKENagguUxywD7IiMuiUBIqRhQ7G5u5sXAUjP0KxA==>. em: 25 nov. 2020.

MANOEL, S. S. **Governança de segurança da informação: como criar oportunidades para o seu negócio**. Rio de Brasport, 2014. Disponível em: <https://plataforma.bvirtual.com.br/Leitor/Publicacao/160684/e code=0NbkAhNFCXQgUoLmIDev0A/8DJIgHgLolYMv2iTAmDOKhpgqkye9ifsA3QaCJGmZRSCpq9nz2GkDkBt534QNuA==>. Acesso em: 25 nov. 2020.

SÊMOLA, M. **Gestão da segurança da informação** - uma visão executiva. 2. ed. São Paulo: Elsevier, 2014.

SILVA NETTO, A.; SILVEIRA, M. A. P. Gestão da segurança da informação: fatores que influenciam sua adoção em pequ médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, [s. l.], v. 4, n. 3, p. 375-397 Disponível em: <https://www.scielo.br/img/revistas/jistm/v4n3/07q01.gif>. Acesso em: 22 nov. 2020.

VERGUEIRO, C. E. A Lei Sarbanes-Oxley e as inovações para a proteção do Mercado de Capitais. **Revista da Faculd Direito, Universidade de São Paulo**, São Paulo, v. 97, p. 305-310, 2002.

PROFISSIONAIS TI. **Governança de TI: Lei Sarbanes-Oxley (SOX) e a TI**. [s. l.], [s. d.]. Disponíve <https://www.profissionaisti.com.br/governanca-de-ti-lei-sarbanes-oxley-e-a-ti> Acesso em: 09 nov 2020.

Gabarito

ATAQUES SINTÁTICOS E SEM NTICOS

No mundo da segurança da informação existem duas classificações específicas para os ataques, sendo eles, os ataques sintáticos e os ataques semânticos, que, combinados, são a origem das conhecidas ameaças compostas ou em inglês composite threats. Considerando essas informações, analise as asserções a seguir e a relação proposta entre elas.

I. Os ataques são divididos em semânticos e sintáticos, sendo que estes últimos são diretos e considerados como um software malicioso, incluindo vírus, worms e cavalo de Tróia.
Porque:
II. Os ataques semânticos são capazes de realizar a modificação e a disseminação de informações corretas e incorretas, com ou sem o uso da tecnologia.

A seguir, assinale a alternativa correta:

a As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I.

É importante o prévio conhecimento dos tipos de ataques existentes bem como a forma em que estão classificadas, pois desta maneira é possível desenvolver uma resposta imediata a qualquer tipo de ataque caso ocorra.

QUALIFICAÇÃO DO PROFISSIONAL DE SEGURANÇA DA INFORMAÇÃO

São muitas as funções da área de segurança da informação e elas são muito dinâmicas, o que exige que os profissionais se atualizem constantemente, para que possam contribuir para a diminuição dos riscos de roubo, perdas e alterações indevidas de informações. Por isso, cada vez mais as empresas demandam não somente formação acadêmica, como também certificações e especializações da área de segurança, além de conhecimento em outras áreas da Tecnologia da Informação.
Fonte: GALVÃO, Michele da Costa. **Fundamentos em segurança da informação**. São Paulo, Pearson, 2015. p.26.

Considerando essas informações, analise as asserções a seguir e a relação estabelecida entre elas:

I. A importância de regras e da formação de comitês responsáveis pelas operações organizacionais exige dos profissionais envolvidos conhecimentos de segurança da informação.
Porque:
II. Esses profissionais precisam conhecer as possíveis ameaças provenientes das ações humanas, envolvendo corrupção e riscos cibernéticos, aos quais esses sistemas de informações empresariais estão sujeitos.

A seguir, assinale a alternativa correta:

b As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.

Para uma atuação eficiente diante aos riscos e desafios pertinentes à segurança das informações, faz-se necessário que o profissional da área possua o prévio conhecimento de áreas ligadas à Tecnologia da Informação, além de certificações e especializações em segurança da informação.