Segurança em Tecnologia da Informação

Prof. Rodrigo Ramos Nogueira
Prof. Rogério Bodemüller Junior

UNIASSELVI
Indaial – 2020
2ª Edição

Elaboração:
Prof. Rodrigo Ramos Nogueira
Prof. Rogério Bodemüller Junior

Revisão, Diagramação e Produção:
Centro Universitário Leonardo da Vinci – UNIASSELVI

Ficha catalográfica elaborada na fonte pela Biblioteca Dante Alighieri
UNIASSELVI – Indaial.

N778s

Nogueira, Rodrigo Ramos

Segurança em tecnologia da informação. / Rodrigo Ramos Nogueira; Rogério Bodemüller Junior. – Indaial: UNIASSELVI, 2020.

190 p.; il.

ISBN 978-65-5663-228-5
ISBN Digital 978-65-5663-225-4

1. Tecnologia da informação. - Brasil. I. Bodemüller Junior, Rogério. II. Centro Universitário Leonardo Da Vinci.

CDD 005.8

Impresso por:

APRESENTAÇÃO

Caro acadêmico, estamos iniciando o estudo da disciplina Segurança em Tecnologia da Informação. Esta disciplina objetiva proporcionar uma aprendizagem autônoma sobre os principais conceitos de segurança na área da tecnologia da informação, proporcionando a você o desenvolvimento de competências necessárias para a implementação da gestão da segurança da informação.

Neste contexto, o Livro Didático de Segurança em Tecnologia da Informação está dividido em três unidades de estudo. A primeira unidade abordará os fundamentos de segurança da informação, apresentando uma introdução sobre porque estudar este tema, definindo e apresentando as propriedades, controles e riscos de segurança da informação, entrando nos principais conceitos sobre segurança lógica, física e ambiental.

Na Unidade 2 serão abordados temas mais técnicos sobre segurança em sistema operacional com as principais vulnerabilidades, técnicas e ferramentas de ataque, inclusive em rede wi-fi, segurança em redes de computadores e segurança da informação na prática.

Na Unidade 3 o foco é mais gerencial, abordando as principais políticas e normas de segurança da informação, a organização da segurança da informação em uma instituição, o controle de acesso e responsabilidades do usuário, finalizando com temas gerenciais sobre a segurança física e do ambiente.

Aproveito a oportunidade para destacar a importância de desenvolver as autoatividades, lembrando que essas atividades NÃO SÃO OPCIONAIS. Elas objetivam a fixação dos conceitos apresentados. Em caso de dúvida na realização das autoatividades, sugiro que você entre em contato com seu tutor externo ou com a tutoria da UNIASSELVI, não prosseguindo as atividades sem ter sanado todas as dúvidas que irão surgindo.

Bom estudo e sucesso na sua trajetória acadêmica e profissional!

Prof. Rodrigo Ramos Nogueira
Prof. Rogério Bodemüller Junior

Você já me conhece das outras disciplinas? Não? É calouro? Enfim, tanto para você que está chegando agora à UNIASSELVI quanto para você que já é veterano, há novidades em nosso material.

Na Educação a Distância, o livro impresso, entregue a todos os acadêmicos desde 2005, é o material base da disciplina. A partir de 2017, nossos livros estão de visual novo, com um formato mais prático, que cabe na bolsa e facilita a leitura.

O conteúdo continua na íntegra, mas a estrutura interna foi aperfeiçoada com nova diagramação no texto, aproveitando ao máximo o espaço da página, o que também contribui para diminuir a extração de árvores para produção de folhas de papel, por exemplo.

Assim, a UNIASSELVI, preocupando-se com o impacto de nossas ações sobre o ambiente, apresenta também este livro no formato digital. Assim, você, acadêmico, tem a possibilidade de estudá-lo com versatilidade nas telas do celular, tablet ou computador.

Eu mesmo, UNI, ganhei um novo layout, você me verá frequentemente e surgirei para apresentar dicas de vídeos e outras fontes de conhecimento que complementam o assunto em questão.

Todos esses ajustes foram pensados a partir de relatos que recebemos nas pesquisas institucionais sobre os materiais impressos, para que você, nossa maior prioridade, possa continuar seus estudos com um material de qualidade.

Aproveito o momento para convidá-lo para um bate-papo sobre o Exame Nacional de Desempenho de Estudantes – ENADE.

Bons estudos!

Olá acadêmico! Para melhorar a qualidade dos materiais ofertados a você e dinamizar ainda mais os seus estudos, a Uniasselvi disponibiliza materiais que possuem o código *QR Code*, que é um código que permite que você acesse um conteúdo interativo relacionado ao tema que você está estudando. Para utilizar essa ferramenta, acesse as lojas de aplicativos e baixe um leitor de *QR Code*. Depois, é só aproveitar mais essa facilidade para aprimorar seus estudos!

BATE PAPO SOBRE O ENADE!

Olá, acadêmico!

Você já ouviu falar sobre o **ENADE**?

Se ainda não ouviu falar nada sobre o ENADE, agora você receberá algumas informações sobre o tema.

Ouviu falar? Ótimo, este informativo reforçará o que você já sabe e poderá lhe trazer novidades.

Vamos lá!

Qual é o significado da expressão ENADE?

EXAME NACIONAL DE DESEMPENHO DOS ESTUDANTES

Em algum momento de sua vida acadêmica você precisará fazer a prova ENADE.

Que prova é essa?

É **obrigatória**, organizada pelo INEP – Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira.

Quem determina que esta prova é obrigatória... O **MEC – Ministério da Educação**.

O objetivo do MEC com esta prova é o de avaliar seu desempenho acadêmico assim como a qualidade do seu curso.

Fique atento! Quem não participa da prova fica impedido de se formar e não pode retirar o diploma de conclusão do curso até regularizar sua situação junto ao MEC.

Não se preocupe porque a partir de hoje nós estaremos auxiliando você nesta caminhada.

Você receberá outros informativos como este, complementando as orientações e esclarecendo suas dúvidas.

Você tem uma trilha de aprendizagem do ENADE, receberá e-mails, SMS, seu tutor e os profissionais do polo também estarão orientados.

Participará de webconferências entre outras tantas atividades para que esteja preparado para #mandar bem na prova ENADE.

Nós aqui no NEAD e também a equipe no polo estamos com você para vencermos este desafio.

Conte sempre com a gente, para juntos mandarmos bem no ENADE!

UNIASSELVI

Olá, acadêmico! Iniciamos agora mais uma disciplina e com ela um novo conhecimento.

Com o objetivo de enriquecer seu conhecimento, construímos, além do livro que está em suas mãos, uma rica trilha de aprendizagem, por meio dela você terá contato com o vídeo da disciplina, o objeto de aprendizagem, materiais complementares, entre outros, todos pensados e construídos na intenção de auxiliar seu crescimento.

Acesse o QR Code, que levará ao AVA, e veja as novidades que preparamos para seu estudo.

Conte conosco, estaremos juntos nesta caminhada!

SUMÁRIO

UNIDADE 1

SEGURANÇA DA INFORMAÇÃO

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- conhecer as principais características de segurança em um ambiente computacional e os principais motivadores de segurança;
- compreender os principais fundamentos de segurança da informação;
- entender a importância dos controles e medidas de segurança lógica, física e ambiental, tendo em vista as diversas vulnerabilidades existentes.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos. No decorrer da unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

TÓPICO 2 – SEGURANÇA LÓGICA

TÓPICO 3 – SEGURANÇA FÍSICA E AMBIENTAL

Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

TÓPICO 1

FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

1 INTRODUÇÃO

Segurança da informação é, de forma sucinta, um conjunto de ações para proteção de um dos mais valiosos ativos em nossa sociedade, a informação. Visando proteger o valor que ele possui, minimizando o risco e o impacto de possíveis ataques. Segurança da informação se aplica em todos os níveis de proteção da informação, independentemente se ela está armazenada em meio digital ou física.

O surgimento das redes de computadores e a interconexão destas aos meios de comunicação expuseram as informações mantidas por estas redes a inúmeros tipos de ataques e vulnerabilidades, dado o valor destas informações e sua importância para as empresas que as geraram e utilizam. O falso anonimato proporcionado por tais meios de comunicação, como por exemplo, a internet, torna ainda mais atrativo para pessoas mal-intencionadas à busca destas informações.

As empresas e instituições das mais diversas naturezas começaram a perceber os problemas relacionados à segurança da informação, e buscam a cada dia mitigar e/ou eliminar os riscos relacionados às vulnerabilidades existentes, protegendo seus dados contra-ataques.

Este tópico, portanto, tem por finalidade apresentar a você os principais conceitos relacionados à segurança da informação, os principais motivadores e os principais benefícios obtidos com a correta utilização de medidas de proteção no ambiente computacional.

2 PORQUE ESTUDAR SEGURANÇA DA INFORMAÇÃO

Historicamente, desde os primeiros homens com a descoberta do fogo, até os segredos industriais das empresas modernas, detinha o poder aquele que possuía a informação. Sun Tzu (2006) já dizia que atacar a estratégia do inimigo é de suprema importância na guerra, seja ela travada pela conquista de uma região, ou de um cliente. A informação, ou a desinformação, faz com que governos e governantes surjam ou mesmo desapareçam. Um grande exemplo disto foi a influência russa na eleição de Donald Trump em 2016 através de uma campanha digital direcionada e por ações de crackers (TIMES, 2016).

Como diz Soares (2014), cada vez mais ouvimos dizer que a informação é o ativo mais importante do século XXI, que a informação é um fator crítico de sucesso, que vivemos em uma sociedade da informação ou que informação é poder. E isto não é novidade, ainda mais hoje, depois de termos passado pela Era Industrial, caracterizada pela revolução industrial e suas industrias, e estarmos na transição entre a Era da Informação e a do Conhecimento, caracterizada pelo bombardeio de dados e informações que recebemos todos os dias por todas os dispositivos tecnológicos que estão ao nosso alcance.

São vários os exemplos de como a informação, ou a falta dela, pode fazer grandes diferenças. A fórmula de como produzir uma Coca-Cola foi, por muitos anos um segredo que manteve a marca entre as maiores do mundo. Outro exemplo são os gigantescos investimentos que as prefeituras estão fazendo para se transformarem em cidades inteligentes, gerando e analisando dados e informações de todas as formas possíveis. Ou ainda os investimentos que as grandes empresas estão fazendo em *big data* como diferencial competitivo. Ou ainda mais próximos de nós, imagine o que poderia acontecer se alguém conseguisse, independentemente como, os dados do seu cartão de crédito.

Um exemplo simples da aplicação da importância de como a informação é o ativo mais importante das organizações, foi o atentado terrorista às Torres Gêmeas em 11 de setembro de 2001. Várias empresas deixaram de existir porque operavam em uma das torres e mantinham seus backups na outra torre (SPANIOL, 2018). Como as duas torres foram abaixo, muitas destas empresas deixaram de existir não por causa da perda física ou de pessoas, e sim por não ter mais as informações que estavam armazenadas por lá. E este não é um caso isolado, há vários casos de empresas que encerraram suas operações porque seus datacenters sofreram por alguma vulnerabilidade, seja lógica, física ou ambiental.

Como um dos maiores crackers dos Estados Unidos nos anos 1990, Kevin Mitnick, hoje consultor de segurança, escreveu:

> Qual é o ativo mais valioso do mundo em qualquer organização? Não é o hardware de computador, não são os escritórios nem a fábrica, nem mesmo o que é proclamado no tão conhecido clichê da corporação – 'Nosso ativo mais valioso é nosso pessoal'. O fato óbvio é que qualquer um deles pode ser substituído. Tudo bem, não tão facilmente, não sem luta, mas muitas empresas sobreviveram depois que sua fábrica foi queimada ou que alguns funcionários chave saíram. Sobreviver à perda da propriedade intelectual, entretanto, é uma história totalmente diferente. Se alguém rouba seus designs de produto, sua lista de clientes, seus planos de novos produtos, seus dados de P&D, esse seria um golpe que poderia fazer sua empresa desaparecer (MITNICK; SIMON, 2005, p. 131).

Apesar do que a mídia define como sendo um hacker, existe uma diferença entre hacker e cracker que estudaremos na Unidade 2. Segundo o Olhar Digital (2013, s.p.):

> Na prática, os dois termos servem para conotar pessoas que têm habilidades com computadores, porém, cada um dos "grupos" usa essas habilidades de formas bem diferentes. Os hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal e nunca invadem um sistema com o intuito de causar danos. No entanto, os crackers têm como prática a quebra da segurança de um software e usam seu conhecimento de forma ilegal, portanto, são vistos como criminosos.

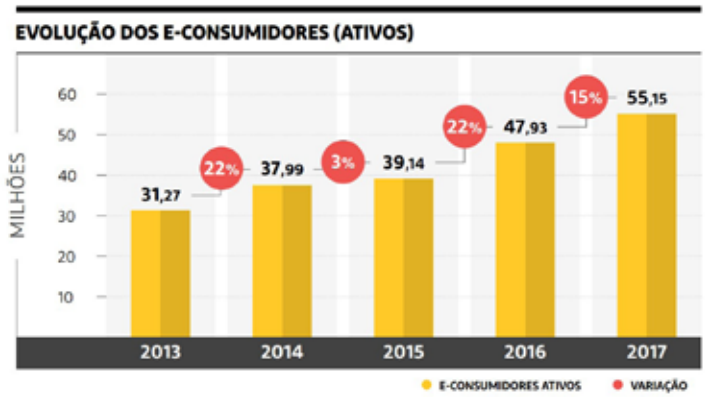
Curioso sobre o mundo hacker? Assista ao seriado *Mr. Robot* da USA Network. Este seriado é um drama, descrito como um suspense tecnológico, no qual um jovem programador que trabalha como engenheiro de segurança cibernética durante o dia e como hacker justiceiro durante a noite. Por mais que seja uma ficção, possui hackers reais trabalhando como consultores e apresenta técnicas e ferramentas reais de *hacking*.

Entendendo o valor das informações, observamos a necessidade de sua proteção, ou seja, a garantia de segurança destas. Mas, como podemos fazer isto? Antes de responder a esta questão, vamos analisar algumas outras informações.

Neste livro, entende-se por informação todo e qualquer conteúdo ou dado que tenha algum valor.

Segundo dados do e-BIT (2018), mais de 55 milhões de consumidores fizeram pelo menos uma compra virtual em 2017, um aumento de 15% se comparado a 2016 ou de 480% se comparado a dez anos antes (9,5 milhões em 2007) ou ainda de 4914% se comparado ao 1,1 milhões de 2001 (e-BIT, 2009).

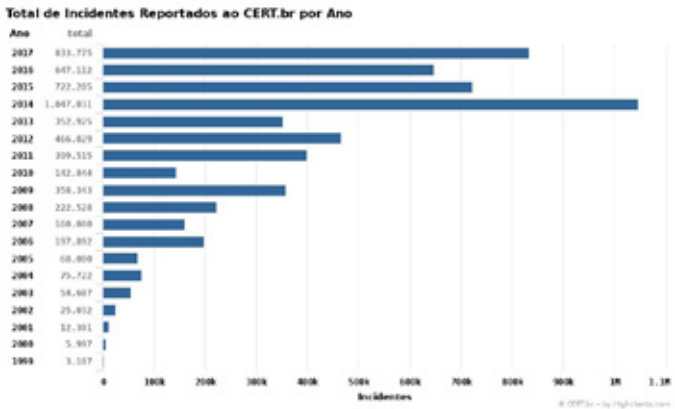
GRÁFICO 1 – EVOLUÇÃO DOS E-CONSUMIDORES (ATIVOS)



FONTE: E-bit (2018, s.p.)

Também podemos observar um crescimento exponencial similar no total de incidentes reportados ao CERT.br, o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. Este levantamento mostra que passou de 12.301 ataques reportados em 2001 para 833.775 em 2017, um aumento de 6678% (CERT.br, 2018a).

GRÁFICO 2 – TOTAL DE INCIDENTES REPORTADOS AO CERT.BR POR ANO



FONTE: CERT.br (2018a, s.p.)

Como podemos analisar com os dados apresentados acima, a expansão da utilização da internet trouxe com ela também o aumento da quantidade de incidentes de segurança, comprovando mais uma vez a necessidade de a segurança ser aplicada na área de tecnologia da informação. Devemos ter em mente que quanto maior for nossa exposição ao mundo digital, maiores serão os riscos digitais que estaremos correndo, se não tomarmos as devidas medidas protetivas. Por exemplo, você possui software antivírus no seu smartphone e em todos seus dispositivos digitais?

Uma maneira simples de entender porque devemos estudar a segurança no mundo digital é através da comparação com os níveis de segurança em atividades comuns. Por exemplo, quando compramos um automóvel, a principal segurança está relacionada com a chave que permite abrir a porta e ligá-lo. Para maior proteção contra os invasores que quebram os vidros, uma prática comum é a instalação de alarmes. Pode-se ainda ter o cuidado de sempre estacionar o automóvel em estacionamentos com vigilantes, além de outros cuidados adicionais. No mundo digital, a segurança funciona de maneira semelhante. Os dados pessoais armazenados em arquivos digitais estão protegidos de acordo com os níveis de segurança utilizados pelos usuários.

Voltando à analogia, mesmo tomando todas as medidas de segurança que você pode, seu automóvel sempre estará 100% seguro? Enquanto você precisa encontrar todas as brechas de segurança e implantar todas as barreiras, um invasor precisaria encontrar uma só brecha desprotegida para ser bem-sucedido. Ou seja, como diz o ditado, "a força de uma corrente é igual à força de seu elo mais fraco".

Todavia, quanto você deve investir em segurança? Você blindaria seu automóvel, contrataria serviço de vigilância via satélite e escolta armada para protegê-lo enquanto fica parado na sua garagem? O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir (BLUEPHOENIX, 2008).

A questão é: existe segurança absoluta? Existe alguma situação em que não existe mais brecha e se está totalmente seguro, sem ameaça alguma ou vulnerabilidade, em que é totalmente impossível acontecer um ataque? A resposta é não! Mesmo sendo utilizado como marketing de alguns produtos, isto não é 100% garantido. Toda segurança é relativa. O que é possível fazer é administrar um nível aceitável de risco.

Acesse o site Segurança Legal (www.segurancalegal.com). Ele possui bons artigos, inclusive um que será apresentado no final desta unidade, e excelentes podcasts (algo como um programa de rádio gravado, ou mesmo uma aula, que você pode ouvir a qualquer hora) que tratam de temas que envolvem Direito da Tecnologia, Segurança da Informação e tecnologia de forma geral.

3 O QUE É SEGURANÇA DA INFORMAÇÃO

A quantidade exponencial de dados que está sendo criada significa que cada ano potencialmente trará brechas de segurança ainda maiores. Mesmo assim, muitas empresas só começam a pensar nisto após terem passado por algum tipo de incidente de segurança. Como já discutimos anteriormente, informação é o ativo mais valioso das grandes empresas e exige uma proteção adequada.

> A informação pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente (ABNT, 2013, p. 6).

O Brasil tem seguido as normas da International Organization for Standardization – ISO, que são publicadas pela Associação Brasileira de Normas Técnicas – ABNT. A norma que trata de gerenciamento de segurança da informação é a ISO/IEC 7799, que foi traduzida e assumiu a sigla ABNT NBR ISO/IEC 17799 (ABNT, 2005). Posteriormente sua atualização, a ISO/IEC 27.002, assumiu a sigla ABNT NBR ISO/IEC 27.002:2013 (ABNT, 2013). Leia esta última para ter um maior domínio sobre as normas de segurança da informação e já se preparar para a Unidade 3.

Segundo o dicionário Houaiss (2018, s.p.), segurança é "estado, qualidade ou condição de quem ou do que está livre de perigos, incertezas, assegurado de danos e riscos eventuais; situação em que nada há a temer". E o que é segurança da informação? "É a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio e maximizar o retorno sobre investimentos e as oportunidades de negócio" (ABNT, 2013, p. 9).

E como conseguir segurança da informação e administrar um nível aceitável de risco já que não existe segurança absoluta?

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio (ABNT, 2013, p. 10).

4 PESSOAS, PROCESSOS E TECNOLOGIAS

Mitnick (2003, p. 4) diz que "a segurança não é um produto, é um processo. Além disso, a segurança não é um problema para a tecnologia, ela é um problema para as pessoas". Isto quer dizer que a segurança possui um conjunto de atividades relacionadas que devem ser executadas em um ciclo contínuo de análise do problema, síntese de uma solução e avaliação da solução.

Segundo Pfleeger (1997), quem investe em segurança da informação deve ter como base três segmentos: pessoas, tecnologia e processos. As pessoas constituem a mais importante variável, mas que muitas vezes é deixada de lado nas organizações. Suas habilidades, atitudes e conhecimentos fazem com que a organização alcance a sua visão de futuro. Sem considerar quem vai executar e interagir, não seria possível definir nem os processos nem as tecnologias.

O processo é a diretriz que organiza e define as ações das pessoas, o caminho de como fazer a organização alcançar seus objetivos. Ele representa como aquela organização funciona, como serão executadas as atividades, por quem será feita esta execução e quais tecnologias serão utilizadas.

Por fim, as tecnologias são as ferramentas que permitem que os processos possam ser executados pelas pessoas, apoiando de forma a alcançar os melhores resultados para a organização. Este talvez seja o mais amplo dos três, pois todo dia é, ou pode ser, criada uma nova ferramenta para executar uma tarefa de uma melhor forma. Se aplicarmos a ideia em segurança da informação, sempre haverá uma nova forma de burlar um sistema.

> Pessoas, processos e tecnologia, trabalhando de forma integrada, acabam por formar o tripé de sustentação, execução e entrega das estratégias corporativas. Assim, quanto maior a aderência e resposta deste tripé às exigências e definições estratégicas da empresa, maior será sua capacidade competitiva da mesma (CORP, 2011, s.p.).

FIGURA 1 – PROCESSO, PESSOAS E TECNOLOGIA

FONTE: Oliveira (2018, s.p.)

A imagem anterior ilustra a importância da integração de pessoas, processos e tecnologia na busca de um ponto de equilíbrio. Caso não haja esta integração, poderá acontecer algum destes casos:

- Processos e tecnologias sem pessoas implica na alienação e alta rotatividade das pessoas e, consequentemente, na subutilização dos sistemas.
- Pessoas e tecnologias sem processos acarreta confusão e um caos automatizado, já que existe um sistema que auxilia em processos não otimizados, além de baixar a qualidade do atendimento ao cliente.
- Pessoas e processos sem tecnologias causa frustração nas pessoas envolvidas e ineficiência nos processos, elevando os custos das operações.

Tenha sempre em mente que segurança da informação é um conjunto que envolve várias variáveis. Do que adiantaria ter um sistema de última geração se os usuários não são treinados para isto. Ou ainda, ter usuários treinados e que seguem processos, mas cujo sistema pode ser invadido por qualquer *script kiddie*. Então, lembre-se de levar em consideração todas estas variáveis em segurança da informação.

Segundo o site sobre tecnologias CanalTech (2014), script kiddie é o nome atribuído de maneira depreciativa aos crackers inexperientes que procuram alvos fáceis para aplicar seus poucos conhecimentos técnicos. Seu objetivo é obter a conta do administrador de uma máquina (root) do modo mais simples possível e que não exija conhecimentos técnicos avançados.

5 AS PROPRIEDADES DE SEGURANÇA DA INFORMAÇÃO

Para proteger a informação, é necessário garantir algumas propriedades. As principais violações destas propriedades, identificadas na literatura, correspondem à revelação não autorizada, modificação e produção não autorizada da informação, além do ataque de negação de serviço (DoS – *Denial of Service*). Evitar estas violações em sistemas complexos é sempre uma tarefa árdua. Segundo a NBR ISO/IEC 27002 (ABNT, 2013) a segurança está fundamentada sobre três propriedades que devem ser mantidas: confidencialidade, integridade e disponibilidade das informações.

- **Confidencialidade**: necessidade de garantir que as informações sejam divulgadas somente àqueles que possuem autorização para vê-las. Ex.: alguém obtém acesso não autorizado ao seu computador e lê as informações contidas na sua declaração de imposto de renda (ZUBEN, 2018).

- **Integridade**: necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas. Ex.: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de imposto de renda, momentos antes de você enviá-la à Receita Federal (ZUBEN, 2018).
- **Disponibilidade**: necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam. Ex.: o seu provedor sofre uma grande sobrecarga de dados ou um DoS e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal (ZUBEN, 2018).

O ataque de negação de serviço, também conhecido como DoS, é uma técnica que visa deixar um sistema indisponível para seus utilizadores. O ataque não é uma invasão ao sistema, ele faz com o sistema seja sobrecarregado de tal forma que não consiga mais cumprir com sua função.

Estes três atributos também são referenciados na literatura como CID (confidencialidade, integridade e disponibilidade), CIA (*availability*, *integrity* e *confidentiality*) ou também como a tríade de segurança (PFLEEGER; PFLEEGER, 2006). Além destes citados, a NBR ISO/IEC 27002 (ABNT, 2013) também define que podem estar envolvidas:

- **Autenticidade**: garante que uma mensagem provém do emissor anunciado e que é livre de adulterações ou qualquer outro tipo de corrupção da mensagem.
- **Não-repúdio**: também chamado de irretratabilidade, é a garantia que o emissor da mensagem não poderá posteriormente negar a autoria da mensagem.
- **Confiabilidade**: é a propriedade de comportamento e resultados pretendidos consistentes, ou seja, é confiável.

A NBR ISO/IEC 27002 utiliza o termo 'não-repúdio', entretanto, a ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) adota o termo 'irretratabilidade' como vernáculo do inglês 'non-repudiation' por se tratar de termo jurídico tradicional, consagrado e amparado pela legislação vigente. As palavras 'repúdio' e 'retratação' referem-se a conceitos distintos no código de direito penal e o primeiro não caracteriza a infração cometida pelo signatário que nega, de má-fé, o compromisso contratual assumido.

Fontes (2006) ainda cita que proteger a informação significa garantir, além das três principais propriedades e do não-repúdio, também as propriedades a seguir:

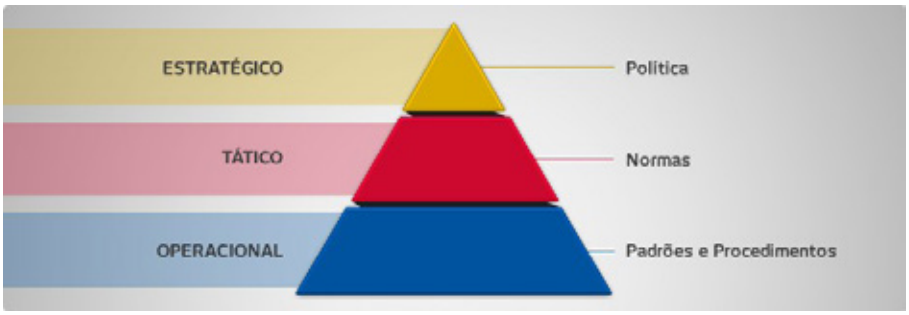
- **Legalidade**: o uso das informações deve estar de acordo com as leis aplicáveis, normas regulamentadoras, licenças, concessões, regimentos e contratos firmados, assim como com os princípios éticos seguidos pela organização e desejados pela sociedade.
- **Auditabilidade**: o acesso e uso das informações devem ser registrados, permitindo identificar quem a acessou e o que este fez com a informação obtida.

Não existe uma hierarquia entre estas propriedades, mas dependendo do objetivo do sistema, podemos perceber uma maior relevância de um sobre os outros. Por exemplo, para acessar seu e-mail, o servidor que hospeda este serviço deve estar **disponível** naquele momento, enquanto que é mais importante que seus dados cadastrais em um serviço devem ser **confidenciais** e ninguém sem autorização possa ter acesso.

6 OS CONTROLES DE SEGURANÇA DA INFORMAÇÃO

Qualidade e segurança andam juntas. Algumas premissas da segurança são originadas nos conceitos que envolvem a qualidade, em que para se obter o desejado, neste caso segurança, é necessário planejamento e envolvimento dos diversos níveis da organização, como podemos observar na imagem a seguir e detalhados em seguida. Obviamente, esta é somente uma introdução para que você possa ter a fundamentação para algumas questões trabalhadas no decorrer desta unidade, mas na Unidade 3 detalharemos um pouco mais algumas políticas, normas, padrões e procedimentos.

FIGURA 2 – POLÍTICA, NORMAS E PROCEDIMENTOS



FONTE: Bradesco (2018, s.p.)

- **Políticas**: utilizadas no nível estratégico, definem a estrutura, as diretrizes e as obrigações referentes à segurança da informação. Um dos principais exemplos é a Política de Segurança da Informação, chamada de PSI, que é um documento que, entre outras coisas, orienta e estabelece as diretrizes para a proteção da informação.

- **Normas**: são utilizadas pelos gerentes no nível tático, estabelecem obrigações e procedimentos, definidos de acordo com as diretrizes da política, a serem seguidos em diversas situações em que a informação é tratada. Um exemplo é a ABNT NBR ISO/IEC 27002 que, dentre outras coisas, normaliza a construção de uma PSI.
- **Procedimentos**: instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades da organização, descrevendo as operações necessárias para a realização de uma tarefa. Hierarquicamente são utilizados no nível operacional. Um grande exemplo são os procedimentos de backups, importantes em várias situações e que devem estar definidas em um documento que especifique o procedimento de controle de backup e restore.

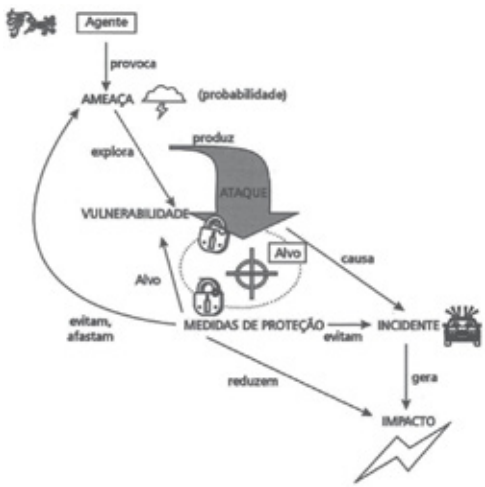
Estes três níveis de controles são definidos e utilizados na mitigação de riscos, ou seja, na busca de prever contra determinada situação, detectar e reagir de forma adequada, buscando diminuir o impacto de um incidente. Estes temas estão definidos a seguir.

7 ANÁLISE E GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

Risco é a combinação da probabilidade de um evento e de suas consequências (ABNT, 2009). Ou, conforme podemos observar na imagem que detalharemos a seguir, de acordo com Sêmola (2003, p. 50):

> é a probabilidade de que agentes, que são ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impactos nos negócios. Esses impactos são limitados por medidas de segurança que protegem os ativos, impedindo que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco.

FIGURA 3 – RELACIONAMENTO ENTRE OS TERMOS ASSOCIADOS AO RISCO PARA A SEGURANÇA DA INFORMAÇÃO



FONTE: Beal (2008, p. 16)

Um exemplo deste fluxo é apresentado na figura anterior. Quando um agente provoca uma ameaça e explora uma vulnerabilidade, produz um ataque ao alvo, causando um incidente de segurança e gerando um impacto. As medidas de proteção podem afastar ou mesmo evitar uma ameaça, proteger o alvo de ataques, evitar os incidentes e reduzir o impacto (BEAL, 2008). Detalharemos melhor estes conceitos nas próximas subseções.

Usando um exemplo de Tusset (2008), vamos começar diferenciando o que são ameaças, vulnerabilidades e ataques através do exemplo de uma casa. Podemos dizer que uma ameaça é o roubo de móveis, dinheiro e eletrodomésticos. Já algumas vulnerabilidades podem ser uma janela aberta ou uma porta que não esteja trancada. E o ataque consiste na invasão propriamente dita com o consequente roubo de bens.

A seguir, alguns outros exemplos apresentados por Lopes (2017):

1- Alguns usuários deixam suas senhas corporativas anotadas na última página da agenda, estas ficam sobre sua mesa de trabalho:
   - Agente: qualquer pessoa.
   - Alvo: agenda.
   - Ameaça: roubo da senha.
   - Vulnerabilidade: ligada ao ativo (agenda, acesso fácil sem controle).
   - Incidente: acessar indevidamente, roubo.
2- Os servidores ficam em uma sala sem controle de temperatura, a rede elétrica não é estabilizada, em caso de falta de energia elétrica não existe redundância e não há um controle de acesso a essa sala:
   - Agente: qualquer pessoa, queda de energia e superaquecimento.
   - Alvo: servidores com os sistemas.
   - Ameaça: roubo dos servidores, indisponibilidade de serviços por falta de energia ou danos causados por alta temperatura.
   - Vulnerabilidade: acesso fácil sem controle.
   - Incidente: roubo dos servidores, indisponibilidade de serviços por falta de energia, queima ou chaveamento automático de equipamentos.
3- Os sistemas operacionais das estações de trabalho não estão atualizados:
   - Agente: agentes mal-intencionados (vírus).
   - Alvo: sistemas, rede interna, aplicativos.
   - Ameaça: instalação de agentes mal-intencionados.
   - Vulnerabilidade: incompatibilidade de sistemas, envio de e-mails, redirecionamento de portas de acesso, acesso remoto indevido, roubo de arquivos ou corrupção deles.
   - Incidente: envio de e-mails, redirecionamento de portas de acesso, acesso remoto indevido, roubo de arquivos ou corrupção deles.
4- A navegação na internet (cabeada e sem fio) não requer autenticação alguma e é liberada:
   - Agente: qualquer pessoa.
   - Alvo: rede.
   - Ameaça: baixo desempenho da navegação.

- Vulnerabilidade: qualquer acesso de qualquer pessoa.
- Incidente: alto consumo de banda, improdutividade no trabalho e infecção da rede.

Os principais componentes descritos anteriormente estão melhor detalhados nas subseções a seguir.

7.1 AMEAÇAS

Uma ameaça é o primeiro ponto a ser estudado por um agente para a concretização de um ataque. Ameaça é a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2013). É qualquer coisa que possa afetar ou atingir o funcionamento, operação, disponibilidade e integridade da rede ou do sistema.

Segundo Beal (2008), as ameaças a que se sujeitam informação e ativos de informação podem ser classificadas como:

- Ambientais: naturais, como fogo, chuva, raio, terremoto, ou decorrentes de condições do ambiente, como interferência eletrônica, contaminação por produtos químicos, falhas no suprimento de energia elétrica ou no sistema de climatização.
- Técnicas: configuração incorreta de componentes de TI, falhas de hardware e software.
- Lógicas: códigos maliciosos, invasão de sistema.
- Humanas: erro de operação, fraude, sabotagem.

Sêmola (2003) também define as ameaças quanto a sua intenção, divididas em três grupos: naturais, involuntárias e voluntárias. A primeira, naturais, refere-se às ameaças decorrentes de fenômenos da natureza. Dentre aquelas que possuem interferência direta do ser humano, as involuntárias são as ameaças inconsistentes, quase sempre causadas pelo desconhecimento e as voluntárias são as ameaças propositais causadas, por exemplo, por crackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador e incendiários.

Sobre as ameaças voluntárias, é importante salientar que não são somente os hackers e crackers que estão motivados a realizar um ataque, mas também funcionários insatisfeitos, ex-funcionários, parceiros de negócio e concorrentes.

Alguns exemplos, não necessariamente da área de tecnologia da informação, mas que podem afetar a segurança da informação são:

- Catástrofes: desabamento, explosão, incêndio e inundação.
- Supressão de serviços: falta de energia, queda de comunicações e falha de equipamentos.

- Comportamento antissocial: paralisações, motins, invasão e piquetes.
- Ação criminosa: terrorismo, sequestro, roubos e furtos, fraudes, sabotagens e espionagem industrial.

A partir do momento em que um agente provocou uma ameaça, independentemente do tipo e da intenção, pode-se explorar alguma vulnerabilidade, que estudaremos na próxima subseção.

7.2 VULNERABILIDADES

As vulnerabilidades são os pontos fracos, ou falhas, existentes e que podem ser explorados em um ataque para gerar um incidente e causar um impacto. Segundo a Cartilha de Segurança para Internet do CERT.br (2018b, s.p.):

> Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Ou seja, a vulnerabilidade por si só não provoca os incidentes de segurança, pois são elementos passivos. Por isto precisam de um agente causador. As suas principais origens são:

- Deficiência de projeto: brechas no hardware/software.
- Deficiência de implementação: instalação/configuração incorreta, por inexperiência, falta de treinamento ou desleixo.
- Deficiência de gerenciamento: procedimentos inadequados, verificações e monitoramento insuficientes.

Alguns exemplos de vulnerabilidades são:

- Instalação física: má proteção física de equipamentos e mídia.
- Hardware e software: situações não previstas, limites e bugs no projeto, deixando brechas que podem ser exploradas.
- Mídia: roubo, perda, danificação, desgaste de discos.
- Transmissão: interceptação de sinal, monitoramento, grampo.
- Humana: desleixo, preguiça, estupidez, ganância, revolta.

Segundo pesquisa da TrendLabs (2012) as dez práticas mais arriscadas feitas por funcionários em empresas são:

- Acessar a internet por redes sem fio desprotegidas.
- Não remover informação confidencial e desnecessária dos computadores.
- Compartilhar senhas com outros.
- Usar o mesmo usuário e senha em diferentes sites e contas on-line.
- Usar dispositivos USB sem criptografia para armazenar informação confidencial.
- Deixar os computadores sem supervisão quando estão fora da empresa.
- Não avisar a empresa após a perda de dispositivos USB com dados confidenciais.

- Não usar telas de proteção ao trabalhar em documentos confidenciais fora da empresa.
- Carregar informação sensível desnecessária no notebook durante viagens.
- Usar dispositivos móveis pessoais para acessar a rede da empresa.

Por mais que esta lista seja de 2012, você considera que ela está desatualizada? Estas práticas estão relacionadas aos procedimentos que as pessoas utilizam e não à tecnologia. Mudar o hábito das pessoas normalmente é mais lento e/ou difícil do que atualizar uma tecnologia.

Analise a imagem a seguir e faça o seguinte exercício: quantas vulnerabilidades você consegue encontrar?

FIGURA 4 – BRECHAS DE SEGURANÇA

FONTE: Peixoto (2006, s.p.)

Nesta imagem vemos uma sala de escritório antiga com funcionários, computadores, mesas, livros e vários outros itens normais de um escritório. Entretanto, várias falhas estão evidentes. Cito algumas: usuário e senha em um *post-it*, um funcionário falando alto a sua senha por telefone, um visitante olhando uma funcionária trabalhar com dados sigilosos, uma caneca de café em cima dos HDs de backup que estão na mesma sala de trabalho, documentos oficiais no lixo padrão, entre várias outras irregularidades que eram inadmissíveis na data de publicação do charge, mas que ainda hoje são praticadas nas empresa.

Pesquise informações sobre as vulnerabilidades da urna eletrônica brasileira, principalmente os artigos relacionados ao Prof. Diego Aranha, analise de forma crítica as informações e tire suas conclusões. Segue uma sugestão de link: <https://www.tecmundo.com.br/seguranca/122152-urnas-eletronicas-falhas-vulnerabilidades-fraudes-mesario.htm>. Acesso em: 25 abr. 2019.

Depois que uma vulnerabilidade foi explorada, um ataque ao alvo acontece. A subseção a seguir apresenta os principais tipos de ataques.

7.3 ATAQUES

Os ataques são o que mais ouvimos falar nas reportagens e abrangem desde um simples vírus até as guerras cibernéticas. Segundo a Cartilha de Segurança para Internet do CERT.br (2018b, s.p.):

> Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

Um ataque a um sistema é uma ação tomada por um intruso malicioso (ou, em alguns casos, um erro de operação por parte de um usuário inocente) que envolve a exploração de determinadas vulnerabilidades de modo a concretizar uma ou mais ameaças (TANENBAUM; WETHERALL, 2011).

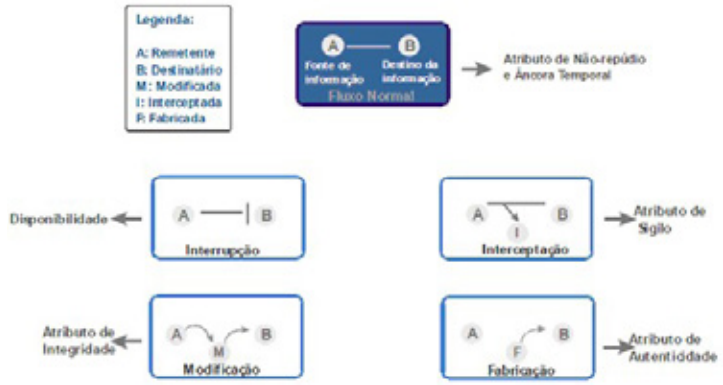
Para entender melhor os ataques, devemos antes entender o modelo de comunicação da teoria da informação de Shannon (1948), ainda aplicado até hoje e que, no seu modelo mais simples, apresenta os seguintes elementos:

- Remetente: responsável por enviar a mensagem.
- Destinatário: a quem a mensagem será enviada.
- Canal de comunicação: por onde a mensagem será enviada.
- Mensagem: a mensagem propriamente dita.

Existem evoluções dela que apresentam um transmissor, um receptor, uma fonte de ruído, um código, entre outros, mas que não serão necessários para este tópico de estudo.

Na figura a seguir é apresentado o fluxo padrão de envio de uma mensagem, alguns possíveis ataques e a relação com os princípios de segurança da informação. Este fluxo normal é aquele que se pretende alcançar em uma comunicação eletrônica segura, em que o remetente A envia a mensagem de forma segura ao destinatário B.

FIGURA 5 – ATAQUES NO ENVIO DE UMA MENSAGEM



FONTE: <https://3.bp.blogspot.com/_y56x_LhbvbA/S8J5KbOJRBI/AAAAAAAAAAc/8csqF8ZuTog/s1600/fluxo.bmp>. Acesso em: 24 abr. 2019.

De acordo com Stallings (2015), apresentado na imagem anterior, os possíveis ataques são:

- **Interrupção**: O fluxo de informação parte do remetente A, mas não chega ao destinatário B, pois é interrompido no meio do caminho. Isto pode ser causado por um impedimento do sistema de informação ou um dano físico às instalações necessárias à transmissão. Um exemplo é quando Alice tenta enviar uma mensagem para Bob, mas a mensagem não chega até ele.
- **Modificação**: O fluxo de informação parte do remetente A, mas é interceptado por um agente malicioso M, que a modifica e envia para o destinatário B. Este tipo de ataque afeta a integridade da informação. Um exemplo deste ataque ocorre quando Alice tenta enviar uma mensagem para Bob, mas antes de ser entregue a mensagem é recebida por um atacante, que a modifica e envia para Bob.
- **Fabricação**: O agente malicioso F entra no circuito de informação e envia uma mensagem ao destinatário B, se passando pelo remetente A, ou seja, a informação é fabricada pelo agente malicioso F e enviada para B. Este ataque afeta a autenticidade da informação. Isto ocorre, por exemplo, quando um atacante envia uma mensagem para Bob, se passando por Aline.
- **Interceptação**: O fluxo de informação parte do remetente A e chega normalmente ao destinatário B, porém o agente malicioso I estava monitorando o fluxo e consegue também ter acesso à informação. Ou seja, a informação é interceptada pelo agente malicioso I sem que A ou B percebam. Este ataque afeta a confidencialidade da informação. Um exemplo é quando Alice envia uma mensagem para Bob, mas um atacante também consegue ler a mensagem.

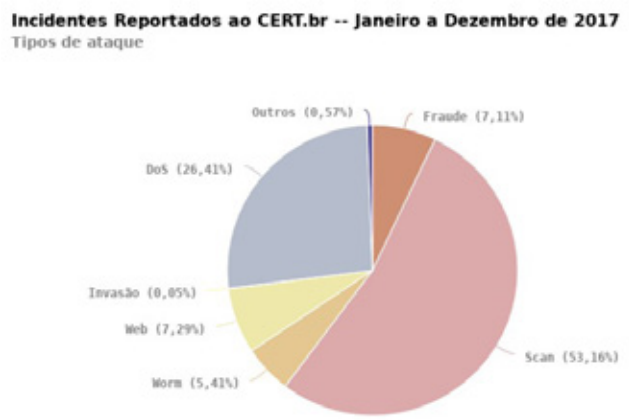
Além disto, outras definições sobre o fluxo da informação é que eles podem ser classificados em dois tipos:

- Passivo: quando só há a interceptação, monitoramento ou análise de tráfego (origem, destino, tamanho, frequência), sem a alteração da mensagem.

- Ativo: quando há adulteração, fraude, reprodução (imitação) ou bloqueio do fluxo da mensagem.

Sobre as formas de ataques digitais, a seguir vemos um gráfico daqueles reportados ao CERT.br no ano de 2017 (CERT.br, 2018a) no qual é possível observar que mais de 50% deles estão relacionados ao escaneamento de portas na busca de brechas para ataques e em segundo lugar estão os ataques de negação de serviço, conhecidos como DoS. Estas portas proporcionam uma interface de entrada e saída para os dados que trafegam na rede. O escaneamento de portas é uma técnica utilizada para procurar por portas abertas em uma rede e desta forma encontrar uma vulnerabilidade.

GRÁFICO 3 – INCIDENTES REPORTADOS AO CERT.BR



FONTE: CERT.br (2018a, s.p.)

Antes de apresentar dois outros ataques que estão causando muito prejuízo às organizações (engenharia social e os ransomware), apresentamos um pouco sobre a segurança na internet que fundamenta uma boa parte dos tipos de ataques.

7.4 SEGURANÇA NA INTERNET

Vamos voltar um pouco no tempo e analisar a charge a seguir, publicada em 1993 no *The New Yorker* (STEINER, 1993). Nela, um cachorro em frente ao computador fala para outro cachorro: "Na internet, ninguém sabe que você é um cão" (tradução livre). Hoje, todo mundo tem pelo menos uma identidade on-line, mesmo que falsa. Qualquer pessoa conectada à internet pode fingir, ser qualquer outra pessoa, seja uma criança, um amigo ou um especialista divulgando notícias alarmantes, sem sequer revelar seu verdadeiro nome. Seja crítico, desconfie e tome as devidas precauções, pois do outro lado pode ser alguém mal-intencionado aplicando de engenharia social para conseguir algo de você.

FIGURA 6 – NA INTERNET, NINGUÉM SABE QUE VOCÊ É UM CÃO

FONTE: Steiner (1993, s.p.)

Em 2015, Hafeez fez uma releitura do cartum anterior, apresentado a seguir. Neste, os mesmos cachorros, ambos mais velhos, observam seu dono no computador quando um pergunta ao outro: "Lembra quando, na internet, ninguém sabia quem você era?" (tradução livre). A charge gera o questionamento se ainda há anonimato on-line. Podemos ainda não saber quem está do outro lado, mas com certeza existem aqueles que sabem. Por exemplo, Edward Snowden apresentou ao WikiLeaks, em 2013, provas de que a Agência de Segurança Nacional dos Estados Unidos da América (NSA) estava vigiando seus próprios cidadãos (G1, 2013). Ou ainda, como disse o ministro de Segurança Pública Raul Jungmann ao TSE em 2018: "Não existe anonimato na internet e a Polícia Federal tem capacidade de chegar a qualquer deles [autores], em qualquer lugar do mundo" (URIBE, 2018).

FIGURA 7 – LEMBRA QUANDO, NA INTERNET, NINGUÉM SABIA QUEM VOCÊ ERA?

FONTE: Hafeez (2015, s.p.)

Acesse o site <https://internetsegura.br/>, idealizado pelo CGI.br (Comitê Gestor da Internet no Brasil) e conheça as cartilhas e jogos didáticos, para todas as idades, que mostram como se manter seguro na internet.

7.5 ENGENHARIA SOCIAL

Sobre engenharia social Mitnick (2013, s.p.) diz: "Uma empresa pode gastar centenas de milhares de dólares em *firewalls*, sistemas de criptografia e outras tecnologias de segurança, mas se um cibercriminoso engana uma pessoa de confiança dentro da empresa, todo esse dinheiro investido não servirá para nada".

Engenharia social se baseia na manipulação psicológica das pessoas, na busca que ela faça o que você deseja. Isto independe de tecnologia e muitas vezes só precisa ter um conhecimento mínimo sobre o assunto. O velho golpe do bilhete premiado, por exemplo, é um ataque de engenharia social. O e-mail com uma história envolvente, que contém um anexo ou um link para você clicar, também se utiliza desse tipo de ataque, e assim a lista vai crescendo, funcionando como base para muitos outros ataques mais complexos. Observe a seguir uma parábola, adaptada, sobre engenharia social, apresentada por Fontes (2006, s.p.).

O ELO MAIS FRÁGIL

Após vários meses de trabalho árduo com a equipe técnica responsável pela proteção dos servidores e da rede, o CIO resolveu contratar uma consultoria externa para tentar quebrar a segurança da empresa. Depois de vários contatos, uma consultoria reconhecida no mercado foi contratada. Os acertos iniciais foram feitos e as regras, acordadas.

Uma semana depois do início do trabalho, os especialistas da consultoria ainda não tinham conseguido entrar no ambiente da rede. O pessoal da organização tinha feito muito bem seu dever de casa.

O prazo para a consultoria estava terminando e nada de quebra de segurança. Até que um dia um dos consultores esqueceu o crachá da organização e teve de esperar no hall de entrada. Ele notou que não havia recepcionista e que os visitantes que chegavam olhavam uma lista de ramais e ligavam para a área de interesse. O funcionário, então, vinha buscar o visitante na recepção. O consultor olhou a lista e logo ligou para o Help Desk de outra unidade solicitando uma nova senha como se fosse um funcionário da empresa. Com um pouco de engenharia social, o atendente aceitou a explicação e forneceu a senha dizendo: "Somos muito rígidos! Essa senha é descartável e você só vai poder utilizá-la uma vez. Sabe como é, são procedimentos de segurança!"

Com um acesso válido, o consultor acessou a rede e, por medida de segurança, trocou a senha descartável. A partir daí foi fácil, pois o consultor tinha-se feito passar por um importante funcionário: o administrador da rede. A consultoria conseguiu mostrar, dentro das regras estabelecidas, a fragilidade na proteção da informação, e a organização recebeu um novo dever de casa para fazer.

Leia o livro *A arte de enganar*, de Kevin Mitnick (MITNICK, 2003). Neste livro o autor conta parte da sua história pessoal e como realizou vários ataques de engenharia social, inclusive contra a própria Agência Central de Inteligência Americana (CIA).

7.6 RANSOMWARE

Enquanto a engenharia social ataca as vulnerabilidades nas pessoas, existe uma vasta gama de ataques que visam a tecnologia. Os ransomwares são um ataque muito utilizado atualmente e que tem provocado grandes prejuízos. Eles são definidos como: "Um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário" (CERT.br, 2018b, s.p.).

Ou seja, um cracker invade seu servidor ou banco de dados, criptografa suas informações e exige um resgate, normalmente pago em alguma moeda digital não rastreável, para liberar a chave que decifra seus dados. Fique atento!

Sequestrar dados de empresas que acabam acarretando prejuízos financeiros é um grande problema, mas há criminosos que estão atacando até mesmo hospitais, colocando vidas em risco. Por este e outros motivos, os ransomwares estão na mira de grandes agências de segurança como, por exemplo, o FBI (FBI, 2018).

Novamente o site <https://cartilha.cert.br/> (CERT.br, 2018b) traz bons esclarecimentos e boas dicas de como se proteger contra este ataque que vem a cada ano acarretando um grande prejuízo financeiro nas organizações, independentemente do tamanho delas.

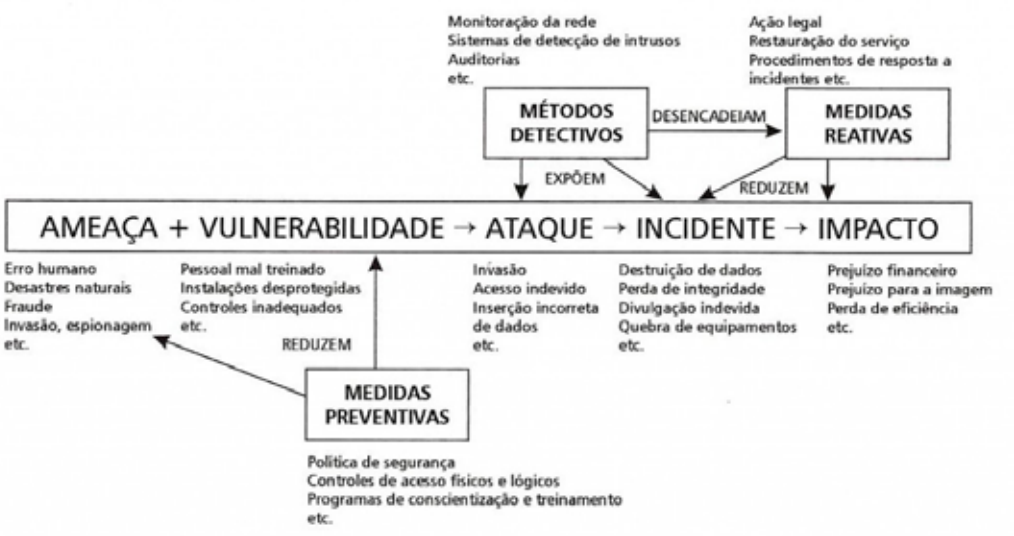
Para afastar ou mesmo evitar uma ameaça, proteger o alvo de ataques, evitar os incidentes e reduzir o impacto, devemos utilizar de algumas medidas protetivas. Estas medidas são apresentadas na subseção a seguir.

7.7 MEDIDAS PROTETIVAS

Existem várias formas de diminuir o risco de segurança da informação. As medidas protetivas são técnicas ou métodos usados para se defender de ataques, ou para fechar ou compensar vulnerabilidades. Segundo Beal (2008), apresentados na figura a seguir, eles podem ser classificados em:

- **Medidas preventivas**: cujo objetivo é evitar que os incidentes venham a ocorrer, são controles que reduzem as probabilidades de uma ameaça e vulnerabilidade, tais como políticas de segurança, controles de acesso físicos e lógicos, programas de conscientização e treinamento e sistemas de prevenção de intrusão.
- **Métodos detectivos**: buscam identificar condições ou indivíduos causadores de ameaça, estes métodos detectam e expõem ataques/incidentes e desencadeiam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita, tais como monitoração da rede, sistemas de detecção de intrusos, auditorias ou até mesmo as câmeras de segurança.
- **Medidas reativas**: que são ações voltadas à correção da estrutura para que se adapte às condições preventivas, reduzem o impacto de um incidente. São medidas tomadas após a ocorrência do evento, tais como ações legais, restauração do serviço e procedimentos de resposta a incidentes.

FIGURA 8 – COMPONENTES DO RISCO E MEDIDAS DE PROTEÇÃO USADAS PARA REDUZI-LO



Componentes do risco e medidas de proteção usadas para reduzi-lo.

FONTE: Beal (2008, s.p.)

Além dos conceitos acima descritos, a imagem também demonstra que as ameaças somadas às vulnerabilidades, quando mal gerenciadas, facilitam o ataque a um ativo da informação e, caso seja concluído, gera o incidente de segurança que culmina em um impacto para os negócios da organização (PRATA, 2009).

Descrição da figura: além do que foi apresentado no texto, a figura exemplifica os seguintes conceitos, já definidos e apresentados nas seções anteriores:

- **Ameaça**: erro humano, desastres naturais, fraude, invasão espionagem etc.
- **Vulnerabilidade**: pessoal mal treinado, instalações desprotegidas, controles inadequados etc.
- **Ataque**: invasão, acesso indevido, inserção incorreta de dados etc.
- **Incidente**: destruição de dados, perda de integridade, divulgação indevida, quebra de equipamentos etc.
- **Impacto**: prejuízo financeiro, prejuízo para a imagem, perda de eficiência etc.

Estas medidas protetivas podem variar de atitudes mais simples, executadas em seu computador e dispositivos móveis, como listado a seguir (CERT.br, 2018b):

- Mantenha os programas instalados com todas as atualizações aplicadas.
- Use apenas programas originais.
- Use mecanismos de proteção.
- Use as configurações de segurança já disponíveis.
- Seja cuidadoso ao manipular arquivos.
- Proteja seus dados.
- Mantenha seu computador/celular com a data e a hora corretas.
- Crie um disco de recuperação de sistema.
- Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros.
- Seja cuidadoso ao enviar seu computador/celular para serviços de manutenção.
- Seja cuidadoso ao utilizar seu computador/celular em locais públicos.
- Tome cuidado ao usar computadores de terceiros.
- Faça backups.
- Utilize sempre boas senhas.
- Utilize sempre que possível a criptografia.

Além destas técnicas e mecanismos mais simples, existem aqueles mais complexos e técnicos, como apresentado no quadro logo a seguir.

Mecanismos de segurança específicos - podem ser incorporados a fim de oferecer alguns dos serviços de segurança.

- Codificação: o uso de algoritmos matemáticos para transformar os dados para um formato que não seja prontamente inteligível. A transformação e subsequente recuperação dos dados depende de um algoritmo e zero ou mais chaves de encriptação.
- Assinatura digital: dados anexados a (ou uma transformação criptográfica de) uma unidade de dados que permite que um destinatário dela prove sua origem e integridade e a proteja contra falsificação (por exemplo, pelo destinatário).
- Controle de acesso: uma série de mecanismos que impõem direitos de acesso aos recursos.
- Integridade de dados: uma série de mecanismos utilizados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.
- Troca de autenticação: um mecanismo intencionado a garantir a identidade de uma entidade por meio da troca de informações.
- Preenchimento de tráfego: a inserção de bits nas lacunas de um fluxo de dados na rede para frustrar as tentativas de análise de tráfego.
- Controle de roteamento: permite a seleção de determinadas rotas fisicamente seguras para certos dados e mudanças de roteamento, sobretudo quando uma brecha de segurança é suspeitada.
- Notarização: o uso de um terceiro confiável para garantir certas propriedades de uma troca de dados.

Mecanismos de segurança difusos: mecanismos que não são específicos a qualquer serviço.

- Funcionalidade confiada: aquilo que é percebido como sendo correto com relação a alguns critérios (por exemplo, conforme estabelecido por uma política de segurança).
- Rótulo de segurança: a marcação vinculada a um recurso (que pode ser uma unidade de dados) que nomeia ou designa os atributos de segurança desse recurso.
- Detecção de evento: detecção de eventos relevantes à segurança.
- Trilha de auditoria de segurança: dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança, que é uma revisão e exame independentes dos registros e das atividades do sistema.
- Recuperação de segurança: lida com solicitações de mecanismos, como funções de tratamento e gerenciamento de eventos, e toma medidas de recuperação.

FONTE: Stallings (2015, p. 15)

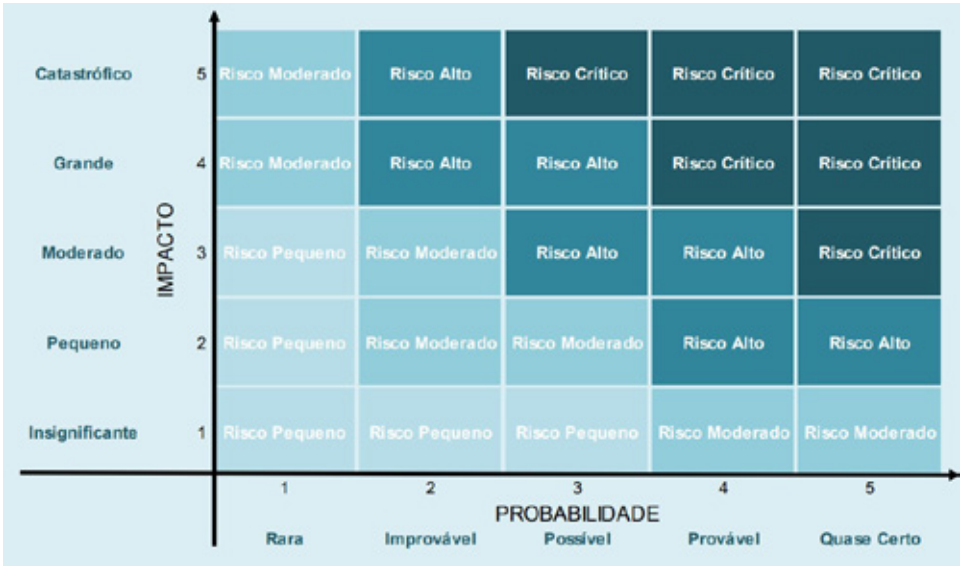
Acesse o site <https://www.cert.br/docs/palestras/> do próprio CERT.br. Neste site, você pode encontrar várias palestras, tanto os slides quanto os vídeos, feitas pelo grupo em vários eventos nacionais e internacionais.

Após a introdução de alguns importantes conceitos relacionados com a problemática da análise e gestão do risco, na subseção a seguir é apresentada uma ferramenta que possibilita rapidamente verificar quais são os riscos que devem receber mais atenção.

7.8 MATRIZ DE RISCO

A matriz de riscos é uma ferramenta que classifica, qualitativamente, os pesos de impacto e probabilidade. Como apresentado na figura a seguir, é particionada em quatro áreas, as quais caracterizam os níveis de riscos (pequeno, moderado, alto e crítico), relacionando com os cinco graus de impacto do incidente (insignificante, pequeno, moderado, grande e catastrófico) e com os cinco níveis de probabilidade de ocorrer (raro, improvável, possível, provável e quase certo).

GRÁFICO 4 – MATRIZ DE RISCO



FONTE: MP (2016, p. 33)

Usando a matriz de riscos em um projeto:

Agora, para vermos na prática como a matriz de riscos funcionaria no gerenciamento de riscos de um projeto, vamos imaginar um projeto de implementação de um novo software em uma empresa. Neste caso, todos os dados de clientes, fornecedores, bem como de pedidos e vendas estão armazenados no sistema antigo (sem backup na nuvem) que vai ser 100% alterado. Vamos ver como seria o passo a passo.

Passo 1 – Liste os principais riscos identificados

Essa é uma breve lista de riscos que poderiam ocorrer ao longo desse projeto:

- Incêndio do data center (com perda de todos os dados).
- Perda de informações essenciais (por erro de um programador).
- Sistema de acompanhamento das novas implementações falhas (impossibilitando registros).
- Falta de compatibilidade entre dados antigos e sistema novo (gerando falhas).
- Falta de qualidade do serviço prestado pela empresa contratada (atrasos, programação ruim etc.).
- Reclamações de usuários por bugs (durante a mudança).
- Aviso tardio aos usuários sobre mudanças (gerando confusão).
- Sistema fora do ar (durante a mudança).
- Ajustes não realizados dentro do prazo (prolongando reclamações e experiência ruim de clientes).
- Quebra de contrato com nova empresa (ocasionando uma perda de tempo e dinheiro).

Passo 2 – Faça a matriz de riscos de cada risco

Ao fazer a matriz de riscos para cada um dos itens elencados, você vai gerar um nível de risco para cada um deles, também podendo gerar uma pontuação de acordo com os pesos que você define para cada nota. Costuma-se adotar uma pontuação de 1 a 5 para cada um dos eixos.

Risco	Perda de Informações Essenciais
Probabilidade	Média
Impacto	Grave

Neste exemplo, no qual a probabilidade é média e o impacto é grave, a nota para perda de informações essenciais seria 12 (3 x 4) de 25 (maior nível de risco possível).

Passo 3 – Analise os riscos mais relevantes em um ranking

Um cuidado importante é não gastar tempo com riscos muito pouco relevantes para o seu projeto. Por isso, depois de utilizar a matriz de riscos, faça a seleção dos riscos mais importantes. Veja que foram separados apenas 5 dos 10 que havia listado em um primeiro momento:

Informações sobre os controles de risco			
Descrição	**Qual etapa?**	**Possível solução para o riso**	**Observação – Matriz de Risco**
Incêndio no Data Center	Backup de informações	Backup prévio	Chance de ocorrer baixa; Impacto gravíssimo
Perda de informações essenciais	Backup de informações	Contratação de empresa para segurança dos dados	Chance de ocorrer média; Impacto grave
Falta de compatibilidade entre dados antigos e sistema novo	Implementação de novo software	Alinhamento com empresa fornecedora do novo software	Chance de ocorrer média; Impacto médio
Reclamações de usuários por bugs	Implementação de novo software	Alinhamento com empresa fornecedora do novo software	Chance de ocorrer alta; Impacto leve
Ajustes não realizados dentro do prazo	Acompanhamento de uso e ajustes	Alinhamento com empresa fornecedora do novo software	Chance de ocorrer baixa; Impacto médio

Passo 4 – Trace medidas para evitar que os riscos se concretizem

A partir de agora que você pode mostrar a qual etapa cada risco está atrelado, bem como listar uma série de soluções que podem ser realizadas para minimizar a chance de o risco acontecer ou para que diminua seu impacto caso o risco se concretize de fato.

Para o risco de falta de compatibilidade entre dados antigos e o sistema novo, uma solução simples são reuniões de alinhamento entre as empresas para que todos os pontos mais importantes sejam contemplados na migração.

Passo 5 – Realize novas medições periodicamente

O último passo do gerenciamento de riscos é o acompanhamento constante. Dependendo do tamanho do projeto ele pode ser realizado a cada etapa entregue, mensalmente ou de acordo com o cronograma do mesmo. O mais importante é ter a certeza de que não esqueceu de todos os riscos que podem impactar negativamente o seu projeto.

FONTE: Ávila (2015, s.p.)

Dentre os pontos fortes da matriz de risco estão a sua simplicidade de cálculo, a determinação e a praticidade de sua aplicação, sobretudo por aqueles que possuem um alto conhecimento prático das situações de risco. Entretanto, a aplicação dela fica comprometida quando a sua não possui um conhecimento aprofundado do problema analisado. Desta forma, ao fazer a análise dos riscos, busque conhecer todas as variáveis envolvidas em todos os cenários possíveis.

RESUMO DO TÓPICO 1

Neste tópico, você aprendeu que:

- É importante a utilização correta da segurança da informação.
- Deve-se levar em consideração as principais características da segurança da informação, em um ambiente computacional.
- Deve haver um equilíbrio entre os processos, tecnologias e pessoas.
- As principais propriedades de segurança da informação são: confidencialidade, integridade, disponibilidade, autenticidade, não-repúdio, confiabilidade, legalidade e auditabilidade.
- Os controles de segurança da informação são: políticas, normas e procedimentos.
- Para garantir a proteção dos ativos, deve-se diminuir os riscos, vulnerabilidades e as ameaças inerentes ao sistema de informação através de medidas de segurança.
- Deve-se realizar a análise dos possíveis riscos e o tratamento deles.
- A matriz de risco pode ser utilizada para a mitigação dele.

AUTOATIVIDADE

Utilize o cenário a seguir descrito para responder as questões desta autoatividade.

(ENADE 2008 - Adaptado) A Secretaria de Saúde de determinado município está executando um projeto de automação do seu sistema de atendimento médico e laboratorial, atualmente manual. O objetivo do projeto é melhorar a satisfação dos usuários com relação aos serviços prestados pela Secretaria. O sistema automatizado deve contemplar os seguintes processos: marcação de consulta, manutenção de prontuário do paciente, além do pedido e do registro de resultados de exame laboratorial. A Secretaria possui vários postos de saúde e cada um deles atende a um ou mais bairros do município. As consultas a cada paciente são realizadas no posto de saúde mais próximo de onde ele reside. Os exames laboratoriais são realizados por laboratórios terceirizados e conveniados. A solução proposta pela equipe de desenvolvimento e implantação da automação contempla, entre outros, os seguintes aspectos:

- sistema computacional do tipo cliente-servidor na web, em que cada usuário cadastrado utiliza login e senha para fazer uso do sistema;
- uma aplicação, compartilhada por médicos e laboratórios, gerência o pedido e o registro de resultados dos exames. Durante uma consulta o próprio médico registra o pedido de exames no sistema;
- uma aplicação, compartilhada por médicos e pacientes, permite que ambos tenham acesso aos resultados dos exames laboratoriais;
- uma aplicação, compartilhada por médicos e pacientes, que automatiza o prontuário dos pacientes, em que os registros em prontuário, efetuados por cada médico para cada paciente, estão disponíveis apenas para o paciente e o médico específicos. Além disso, cada médico pode fazer registros privados no prontuário do paciente, apenas visíveis por ele;
- uma aplicação, compartilhada por pacientes e atendentes de postos de saúde, que permite a marcação de consultas por pacientes e(ou) por atendentes. Esses atendentes atendem o paciente no balcão ou por telefone.

1 (TRE-CE 2011 – Adaptado) Um ponto muito importante e que deve ser levado em consideração nesta solução, mesmo porque ela irá tratar com dados privados e extremamente sensíveis, é a segurança da informação. Sobre este tema, avalie as afirmações a seguir:

I- É obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

II- Os controles de segurança precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.
III- É importante para os negócios do setor público para proteger as infraestruturas críticas, mas não no setor privado. A função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-Gov) e evitar ou reduzir os riscos relevantes.

Assinale a alternativa CORRETA:
a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas I e III estão corretas.
c) ( ) As afirmativas II e III estão corretas.
d) ( ) A afirmativa I está correta.

2 (SEFAZ-RS 2014 – Adaptado) Na segurança da informação, vários componentes estão envolvidos na gestão de riscos, tais como os agentes, as ameaças e os ataques. A fragilidade de um ativo, como os servidores que hospedam o sistema da Secretaria da Saúde, que pode ser explorada por uma ou mais ameaças, é chamada de:

a) ( ) Risco.
b) ( ) Incidente.
c) ( ) Ameaça.
d) ( ) Vulnerabilidade.

3 (SEFAZ-RS 2014 – Adaptado) Vários conceitos permeiam na análise e gestão de riscos em segurança da informação, tais como ameaças, vulnerabilidades, ataques, medidas protetivas, entre outros. No antigo sistema da Secretaria da Saúde, existia a fragilidade do armazenamento dos registros em papel que poderiam, por exemplo, serem queimados por um incêndio iniciado por um curto-circuito. A fragilidade deste ativo, que pode ser explorada por uma ou mais ameaças, é chamada de:

a) ( ) Risco.
b) ( ) Incidente de segurança da informação.
c) ( ) Desastre.
d) ( ) Vulnerabilidade.

4 (ENADE 2011 – Adaptado) Em um determinado momento, o servidor que hospeda o sistema da Secretaria de Saúde recebe uma quantidade de requisições de operações, vindas de números IPs distintos, muito acima das condições operacionais previstas para os seus recursos e "trava", isto é, os seus serviços são interrompidos. Muitas empresas e entidades governamentais sofrem esse tipo de ataque hacker. Para realizá-lo, um atacante precisa distribuir um código, em vários computadores, normalmente

sem o consentimento dos destinatários, que se tornam seus "zumbis". Em um momento, o atacante ativa os "zumbis" que fazem muitos acessos a um determinado alvo, acabando por esgotar seus recursos e derrubando o sistema de informações. A respeito do ataque que o sistema da Secretaria de Saúde foi alvo, analise as afirmações a seguir:

I- É um ataque de negação de serviço (*Denial Of Service*).
II- É um ataque que ameaça o atributo da disponibilidade do sistema.
III- É um ataque em que os hackers roubam as senhas dos usuários, para poder enviar requisições.
IV- É um ataque não detectável por sistemas de antivírus.

Assinale a alternativa CORRETA:
a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas I e IV estão corretas.
c) ( ) As afirmativas II e III estão corretas.
d) ( ) As afirmativas III e IV estão corretas.

5 (ENADE 2008 – Adaptado) Considerando que entre os principais benefícios deste projeto de melhoria de sistema de informação destacam-se o aumento da: eficiência (ato de fazer as coisas da maneira certa); eficácia (ato de fazer a coisa certa); integridade; e disponibilidade, avalie as afirmações a seguir:

I- A falta de energia elétrica, por exemplo, poderá levar ao não funcionamento do servidor ou das máquinas clientes web, fazendo com que as informações sobre prontuários, pacientes, consultas e exames fiquem inacessíveis.
II- Falhas de conectividade à internet poderão levar o sistema à indisponibilidade, e impedir que o médico acesse as informações do paciente, que os atendentes marquem consultas, que os laboratórios recebam e processem pedidos de exame etc.
III- Quebra de equipamentos de armazenamento, como discos rígidos e outras mídias, poderão levar a perda de informações sobre pacientes, médicos, exames, laboratórios etc.
IV- Incêndios em postos de saúde poderão prejudicar a restauração do funcionamento destes, pois todos os dados dos pacientes e médicos serão perdidos caso os computadores deste posto de saúde também sofram com o incêndio.

Assinale a alternativa que descreve riscos de segurança da informação que aumentam quando se substitui o sistema atual pelo sistema proposto, e que são relativos à interação entre pacientes e os serviços da referida secretaria de saúde.

a) ( ) As afirmativas I e III estão corretas.
b) ( ) As afirmativas II e IV estão corretas.
c) ( ) As afirmativas I, II e IV estão corretas.
d) ( ) As afirmativas I, II e III estão corretas.

6 (ENADE 2017 – Adaptado) A Secretaria de Saúde sofreu um novo ataque hacker e seus sistemas foram comprometidos. Depois de alguns dias, a equipe de Tecnologia da Informação (TI) da secretaria conseguiu reestabelecer os sistemas, tendo a gestora de TI apresentado um plano com o intuito de criar um setor especializado em segurança da informação para evitar novos ataques. Após a análise dos riscos e benefícios do plano, foi aprovada a implantação do referido setor de segurança da informação. A partir desta especificação do cenário, avalie as asserções a seguir e a relação proposta entre elas.

I- A implantação de um setor de segurança da informação está associada ao desenvolvimento de uma política de segurança da informação, que é um conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários.

PORQUE

II- É interessante verificar a possibilidade de implantação de um sistema que auxilie na preservação da confidencialidade, da integridade e da disponibilidade da informação, por meio da aplicação de um processo de gestão de riscos, fornecendo a confiança de que os riscos são adequadamente gerenciados, sendo importante que este sistema esteja integrado aos processos da organização e a sua estrutura global.

A respeito dessas asserções, assinale a opção CORRETA:

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

TÓPICO 2

SEGURANÇA LÓGICA

1 INTRODUÇÃO

O propósito deste, e do próximo tópico, é demonstrar uma visão da segurança da informação em todos os contextos, de segurança lógica, física e ambiental, de modo a permitir o desenvolvimento e implantação de medidas de segurança que possam proteger as organizações, os geradores das informações e os seus usuários. Estas medidas visam protegê-los dos inúmeros danos que podem ser causados por conta da destruição, acesso, alteração, exclusão ou divulgação indevida destas informações. Sendo que estes danos podem acabar causando sérios prejuízos financeiros, perda de credibilidade no mercado, desvalorização das ações da organização, danos à imagem da corporação ou ainda sanções e penalizações por conta do descumprimento de leis ou cláusulas contratuais de confidencialidade, entre tantas outras.

Conforme Beal (2008) diz, os problemas de segurança da informação são complexos e normalmente têm sua origem em preocupações organizacionais e de negócio, não de tecnologia. Por exemplo, o problema normalmente não está no sistema de gerenciamento de senhas, e sim na norma que exige que a senha seja trocada todo dia, forçando a pessoa a anotar sua senha em algum pedaço de papel que pode ser deixado em qualquer lugar.

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, de que ameaças e por que razão, antes de poder passar à seleção de soluções específicas de segurança física, lógica e organizacional. Segundo Sêmola (2003, p. 18):

A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada.

Analise a parábola a seguir e observe como o mundo de segurança física e lógica da informação pode nos surpreender.

O PERIGO ESTAVA NO AR!

A preocupação com a segurança era normal na empresa. Por mais que o diretor financeiro sempre reclamava um pouco dos gastos com segurança, terminava aprovando a compra de servidores, firewalls e outros programas específicos. Ele sempre perguntava sobre invasões de hackers, mas o técnico o tranquilizava, informando que estavam bem protegidos.

Em um dia pela manhã, tudo parecia normal. O diretor estava com um computador novo, consultando a Internet quando, de repente, seu micro piscou, entrou em outra página e ficou piscando. Um pouco apreensivo, reiniciou o micro. Acessou a Intranet, e o micro começou a entrar em páginas sem ele comandar. "Invasão!", imaginou. Telefonou para o suporte técnico, mas o responsável não tinha chegado. Ele precisava agir rapidamente e, antes que a invasão se alastrasse, mandou uma ordem para a área de operações de computadores: "Desliguem tudo, estamos sendo invadidos! Tomaram conta do meu computador e, em seguida, vão tomar conta da empresa!"

Uma consultoria especializada foi acionada, afinal, tinham um contrato assinado para esse tipo de problema. Ao chegar à empresa, os consultores foram analisar os servidores, os demais micros e o micro do diretor, que os acompanhava com olhos arregalados. Como tudo tinha sido desligado às pressas, alguns procedimentos para salvar informações não tinham sido realizados. Eles começaram pelos servidores e um a um foram sendo novamente ligados.

Aparentemente estava tudo normal, até que acessaram a Intranet no computador do diretor financeiro e o cursor do mouse começou a correr pela tela. Os demais computadores estavam normais. Somente o novo computador do diretor financeiro continuava com problema. Todos olhavam para aquele mistério, até que o técnico falou: "Não estou gostando desse mouse sem fio. Essa Avenida Paulista tem muita coisa misteriosa no ar".

Sendo assim, resolveram colocar um velho mouse via cabo, e a invasão parou! O novíssimo mouse sem fio sofria com as ondas da Avenida Paulista.

FONTE: FONTES, E. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

Como exemplificado, devemos garantir tanto a segurança física quanto a segurança lógica das nossas informações. A primeira será tratada no Tópico 3 desta unidade. A respeito da segunda, segurança lógica, ela irá garantir a segurança dos sistemas e das informações armazenadas em meio digital da organização, fornecendo mecanismos para garantir as propriedades de segurança da informação que são necessários, tais como confidencialidade, integridade e disponibilidade. Por exemplo, pessoas são treinadas para utilização do sistema, processos são definidos a partir de normas, políticas e tecnologias são utilizadas. Segundo Adachi (2004, s.p.), é na camada de segurança lógica que estão as "regras, normas, protocolo de comunicação e onde efetivamente, ocorrem as transações e consultas".

E quais recursos devem ser protegidos? Segundo o TCU (2012), a proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional. E como proteger? Uma característica essencial no meio digital, que permeia todas as grandes áreas de segurança da informação é a criptografia, apresentada na seção a seguir.

2 CRIPTOGRAFIA

Criptografia, do grego Kryptos (ocultar) e grafos (escrever), significa "escrita oculta". O seu uso data do antigo Egito (onde os faraós mandavam ocultar informações sobre os seus tesouros) e foi fundamental nos capítulos mais delicados da história da humanidade. Usada na antiga Roma por Júlio César (50 a.C.), foi sempre arma de militares, diplomáticos e espiões, e é a defesa das comunicações e dos dados que circulam na grande rede que une o mundo, a Internet.

Uma maneira de proteger a informação é feita através da mudança da sua forma, por meio do processo chamado cifragem (ou transformação criptográfica), na qual um texto legível é tornado ilegível. Analogicamente, o processo inverso chama-se decifragem, no qual o texto ilegível, ou cifrado, é tornado legível como na sua forma original.

"A criptografia é a arte e ciência de cifrar e decifrar mensagens de maneira a estabelecer um canal de comunicação sigiloso entre as pessoas envolvidas na troca de informação" (GILL, 2002, s.p.) e se baseia no que é chamado de Princípio de Kerckhoffs: "O funcionamento interno de um criptossistema não pode ser secreto; deve-se presumir que o adversário conhece como o criptossistema funciona, e a segurança do sistema deve estar na escolha das chaves" (PELLEGRINI, 2018, s.p.).

Ou seja, não pode haver o que se chama por segurança pela obscuridade, que se fundamenta na segurança pelo atacante não saber os detalhes. Evite garantir a segurança de seu sistema somente por esconder algo do atacante. Assim que alguém encontrar isto, o sistema estará comprometido. Ele funciona parecido com o esconderijo das brincadeiras de esconde-esconde onde você se esconde, mas quem procurar bem vai conseguir lhe achar. É só uma questão de tempo.

Por mais que isto seja comum, como Kerckhoffs apresentou no século XIX, isso não garante segurança. Partindo deste princípio, em vez de criar um algoritmo novo e mantê-lo em segredo, confie naqueles que foram largamente testados. Além disto, uma boa prática utilizada por várias empresas de segurança é colocar seus mecanismos de segurança na internet para que sejam atacados, muitas vezes até premiando os melhores, como a Competição Pwn2Own que pagou R$2,5 milhões por 51 falhas em softwares em 2017 (ROHR, 2017).

Lembra no Tópico 1 quando recomendamos que você buscasse informações sobre a segurança da urna eletrônica? A principal crítica feita é que muito do que é utilizado nela é segredo, quando não deveria, segundo vários críticos. Agora que você conhece o princípio de Kerckhoffs datado do no século XIX, analise novamente as informações sobre nossa urna, e as demais utilizadas em outros países, e tire suas conclusões.

2.1 TERMINOLOGIA

Um exemplo da aplicação dos principais conceitos utilizados na criptografia é através da utilização a Cifra de César. Nela, se utilizarmos a chave criptográfica 3 e o texto plano "ABC", o processo de cifragem resultaria no texto cifrado "DEF". Se quiséssemos fazer o inverso, utilizando a mesma cifra e a mesma chave, o processo de decifragem de "DEF" resultaria em "ABC". Os conceitos utilizados neste exemplo estão descritos a seguir.

- Texto plano/original – texto (dado/informação/mensagem) que está no estado não cifrado ou decifrado, texto legível.
- Texto cifrado – texto que foi codificado, saído do processo de criptografia.
- Cifras e códigos – algoritmo criptográfico utilizado para prover confidencialidade à informação, sendo:
  - Código – palavra ou frase é substituído por outra palavra, número ou símbolo.
  - Cifra – age num nível mais fundamental, onde as letras são substituídas.
- Chaves criptográficas – valor numérico ou código usado com um algoritmo criptográfico para transformar, validar, autenticar, cifrar e decifrar dados.
- Cifragem – processo de codificação ou ocultação, transformando o texto claro em um texto cifrado. É o processo de conversação de dados em "código ilegível" de forma a impedir que pessoas não autorizadas tenham acesso à informação.
- Decifragem – processo inverso da cifragem, é o processo que transforma dados previamente cifrados e ininteligíveis de volta a sua forma legível.
- Computacionalmente seguro – quando o custo para quebrar a criptografia excede o valor da informação, ou ainda, quando o tempo para quebrar a criptografia é maior que o tempo de vida da informação.

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar. Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.

O número de chaves possíveis depende do tamanho da chave. Por exemplo, uma chave de 8 bits permite uma combinação de no mínimo 256 chaves (2^8). Quanto maior o tamanho da chave, mais difícil será quebrá-la, pois estaremos aumentando o número de combinações.

2.2 CLASSIFICAÇÃO

O modo como são empregadas as chaves podem ser divididas em criptografia simétrica e assimétrica.

- **Criptografia simétrica** – onde a mesma chave é utilizada para cifrar e decifrar uma mensagem. Estas chaves precisam ser compartilhadas entre o emissor e o receptor por algum outro meio, antes que a comunicação seja firmada.
- **Criptografia assimétrica** – utiliza um par de chaves, uma chave pública e uma chave privada. A chave pública pode ser distribuída livremente, enquanto a chave privada deve ser de conhecimento apenas de seu dono. Uma mensagem cifrada com a chave pública pode somente ser decifrada pela sua chave privada. Do mesmo modo, uma mensagem cifrada com a chave privada pode somente ser decifrada pela chave pública correspondente.

2.3 HASH

O processo de cifragem e decifragem ocupam processamento da máquina e consequentemente demoram um tempo. Para deixar esse processamento mais veloz, em vez de cifrar toda a mensagem, dependendo de qual atributo de segurança que se deseja garantir, é cifrado somente um resumo da mensagem. Segundo Stinson (2002), função resumo, ou *hash*, é usada para construir uma pequena impressão digital de algum dado; se o dado for alterado, então a impressão digital não será mais válida.

2.4 ASSINATURA DIGITAL

Uma das aplicações para o *hash* são as assinaturas digitais. A assinatura digital garante que o receptor da mensagem possa confirmar se assinatura do emissor é autêntica (autenticidade), garante que a mensagem realmente provém de determinado remetente (não-repúdio) e garante que a mensagem não foi adulterada (integridade). Volte no modelo de comunicação da teoria da informação de Shannon (1948), no Tópico 1, seção 7.3, e observe os benefícios que a assinatura digital pode trazer.

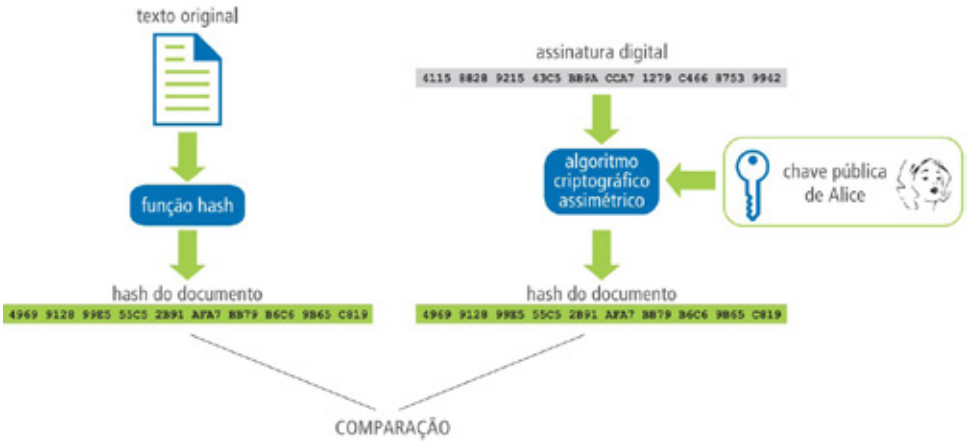
Para criar uma assinatura digital para uma determinada mensagem, deve-se calcular o *hash* dela, após isso, cifrar este *hash* com a chave privada do emissor e então enviar junto com a mensagem original, como apresentado na figura a seguir.

FIGURA 9 – HASH

FONTE: ITI (2012, s.p.)

Para verificar a assinatura, é necessário primeiramente decifrar a assinatura digital com a chave pública do emissor, depois calcular o *hash* da mensagem recebida e comparar os resultados, como apresentado na figura a seguir. Se forem iguais, a assinatura é válida.

FIGURA 10 – ASSINATURA DIGITAL



FONTE: ITI (2012, s.p.)

2.5 CERTIFICADO DIGITAL

Uma das formas mais tradicionais de se utilizar a assinatura digital é através dos certificados digitais. São eles, por exemplo, que permitem a comunicação segura em páginas HTTPS (aquelas que têm o cadeado na barra de navegação do seu browser), onde uma sessão SSL (*Secure Sockets Layer*) é estabelecida sobre a conexão TCP (*Transmission Control Protocol*), entre o programa navegador do usuário e o servidor. Além das características adquiridas pela assinatura digital, o SSL também utiliza da criptografia simétrica para transmitir os dados de forma confidencial.

Enquanto no mundo físico uma carteira de identidade é emitida por um órgão confiável e contém um conjunto de informações que identificam o seu dono, no mundo virtual é o certificado digital que faz essa função. Segundo Fernandes

(2001), um certificado digital pode ser definido como um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

Acesse o site <https://www.iti.gov.br/icp-brasil> e conheça a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), há uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Para saber mais sobre como funciona o processo de assinatura digital, acesse a cartilha "O que é certificação digital?" (ITI, 2012), também do ITI (Instituto Nacional de Tecnologia da Informação), disponível em: <http://antigo.iti.gov.br/servicos/158-publicacoes/cartilhas>. Acesso em: 26 abr. 2019.

2.6 HISTÓRIA DA CRIPTOGRAFIA CLÁSSICA

Podemos chamar de criptografia clássica o período que vai desde os povos antigos, passando pela Idade Média e chegando até as máquinas eletromecânicas, utilizadas principalmente durante a Segunda Guerra Mundial.

Dentre as cifras clássicas mais conhecidas, temos o scytale espartano, a de César e a de Vigenère. E como máquina eletromecânica, temos a Enigma.

Acesse o site e conheça um pouco da história da criptografia.

Você já ouviu falar de Alan Turing, o pai da computação e responsável pela quebra da máquina Enigma utilizada na Segunda Guerra Mundial? Assista ao filme *O Jogo da Imitação*, de 2014, da produtora Diamond Films.

2.7 EXEMPLOS DE CIFRAS CLÁSSICAS

Vamos estudar agora alguns exemplos do processo de cifragem utilizando a criptografia simétrica. Lembre-se de que neste caso, para decifrar, é só realizar o processo inverso.

Cifra de César

Começamos com a cifra de César, uma cifra de substituição que troca cada letra por outras três posições a frente no alfabeto, assim o A é substituído pelo D, o B pelo E, assim por diante. Segue um exemplo:

- Texto plano: SEGURANCA DA INFORMACAO
- Chave: 3
- Texto cifrado: VHJXUDQFD GD LQIRUPDFDR

Cifra de Vigenère

A cifra de Vigenère é uma cifra por substituição polialfabética, na qual a chave deixa de ser a quantidade de posições para ser uma sequência de letras, utilizando a cifra de substituição uma letra por vez. A seguinte grade é utilizada para esta cifra, na qual a linha define a letra do texto plano, a coluna, a letra da chave e, a união das duas, o texto cifrado.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Descrição da figura: é um quadro de 27 linhas por 27 colunas com as letras do alfabeto distribuídas nas células do quadro. A primeira célula da primeira coluna está em branco. A primeira linha e a primeira coluna servem como título, onde a primeira linha tem o alfabeto de A à Z, uma letra por célula, iniciando na segunda coluna, e a primeira coluna tem o mesmo formato, com as letras de A à Z a partir da segunda linha. A segunda linha é igual a primeira, com exceção da primeira coluna. A partir desta, cada linha é igual a sua anterior, mas cada letra tem um deslocamento de uma letra. Assim, a terceira linha inicia em B, passa todo o alfabeto até chegar no Z e finaliza com a letra A. A quarta linha inicia em C, passa por todo o alfabeto e finaliza em B e assim por diante.

Nesta cifra, a letra B se transformaria em B se utilizasse a chave A, em L se utilizasse a chave K e em A se utilizasse a chave Z. Uma característica desta cifra é que ela se comporta como a cifra de César se for utilizado como chave uma sequência de letras D, por exemplo, utilizando a chave DDD a sequência ABC se transformaria em DEF, assim como acontece na cifra de césar. A complexidade está no fato que a chave poderá ser um texto e não somente uma letra. Segue um exemplo de sua utilização:

- Texto plano: SEGURANCA DA INFORMACAO
- Chave: UNIASSELVI
- Texto cifrado: MROUJSRNV LU VVFGJQLXII

Máquina Enigma

Já a máquina Enigma, que teve várias versões, também era uma cifra de substituição polialfabética, mas utilizava uma série de configurações para produzir o texto cifrado. Segue um exemplo utilizando o modelo Enigma I:

- Texto plano: SEGURANCA DA INFORMACAO
- Refletor: UKW A
- Rotor 1: posição 1 + anel 1
- Rotor 2: posição 17 + anel 1
- Rotor 3: posição 12 + anel 1
- Painel: un ia se lv
- Texto cifrado: LKNXXHZHF FE BPLPMHDMRJ

Cerca de Ferrovia

Com o nível de complexidade similar das cifras de substituição, existem as cifras de transposição. Estas consistem no reordenamento das letras a partir de um esquema. A cerca de ferrovia, por exemplo, separa elas em duas linhas diferentes, e depois uni a primeira linha com a segunda. Por exemplo:

- Texto plano: SEGURANCA DA INFORMACAO

- Transformação:

S G R N A A N O M C O
E U A C D I F R A A

- Texto cifrado: SGRNAANOMCOEUACDIFRAA

Leia o livro *O Livro dos Códigos de Singh* (2001). Ele conta de uma forma leve e descontraída a história da segurança da informação, partindo de 500 a.C. até os dias atuais com a criptografia pós-quântica, apresentando várias cifras, suas características e suas utilizações.

A criptografia fornece uma importante medida protetiva, mas se utilizada sozinha, não será suficiente. De nada adianta a tranca da porta da sua casa ser difícil de ser arrombada se você deixa a chave debaixo do tapete. Além da criptografia, deve existir um controle de acesso às chaves criptográficas. Na próxima seção estudaremos os mecanismos de segurança específicos utilizados para isto.

3 MECANISMOS DE AUTENTICAÇÃO

Segundo Goodrich e Tamassia (2013), os mecanismos de autenticação determinam a identidade de alguém ou o seu papel dentro daquele sistema, sendo que essa determinação pode ser feita de diversas maneiras diferentes. Geralmente esta determinação será baseada em uma combinação de:

- algo que a pessoa sabe – como uma senha;
- algo que a pessoa possui – como um cartão inteligente ou um dispositivo que armazena chaves secretas;
- algo que a pessoa é ou faz – como sua impressão digital ou assinatura.

Veremos nas próximas subseções estes três tipos de mecanismos. Iniciamos a seguir com o mais tradicional destes.

3.1 SENHAS

Este tipo de mecanismo de autenticação abrange tudo aquilo que o usuário sabe. Alguns exemplos deste meio de autenticação da identidade do usuário são uma senha, um número de identificação pessoal (PIN) ou respostas a um conjunto de perguntas pré-estipuladas (STALLINGS, 2015).

Segundo o CERT.br (2018b), uma senha, ou *password*, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a simplicidade que possui. Algumas vantagens na sua utilização são:

- onde o usuário estiver, a senha estará com ele;
- a senha pode ser facilmente modificada, se necessário;
- a senha é facilmente inserida através do teclado, não necessitando de dispositivos especiais.

Entretanto, entre outras coisas, uma senha pode:

- ser copiada, caso seja anotada em um post-it do lado do computador, por exemplo;
- ser esquecida, já que devemos lembrar de muitas senhas e números;
- ser adivinhado por uma pessoa não autorizada (*password guessing*), caso seja utilizado alguma senha simples como veremos mais a seguir;
- sofrer um ataque do dicionário (*dictionary attack*), no qual o atacante utiliza palavras armazenadas em um dicionário digital;
- ser comprometida através de engenharia social, como quando um atacante se passa como sendo funcionário do seu banco e liga para você pedindo informações confidenciais;
- ser descoberta através de *keylogger*, é um programa criado para gravar tudo o que é digitado em um teclado de computador.

Observe a tirinha a seguir na qual uma usuária de computador conversa com um técnico do suporte de TI. Analise como ocorre um conflito de aplicação da segurança da informação.

FIGURA 11 – SISTEMA PROTEGIDO

FONTE: Suporte (2018, s.p.)

Descrição da figura: A figura apresenta quatro quadros nos quais o seguinte diálogo ocorre:

- Usuária: Alguém sem autorização acessou o sistema da minha máquina e roubou informações confidenciais.
- Suporte: O sistema estava protegido com uma senha forte?
- Usuária: Sim.
- Suporte: Certeza?
- Usuária: Absoluta!
- Usuária: É uma senha tão complicada que até precisei anotar num post-it e colar aqui no monitor. Olha…

Vamos para um exemplo um pouco mais complexo, mas que acaba terminando em um ponto simples. Você precisa enviar um e-mail sigiloso para alguém utilizando a assinatura digital, mas não possui um certificado digital para gerar esta assinatura, então resolve utilizar uma plataforma de e-mail criptografado. Entretanto, por mais que seu e-mail possa ser criptografado, antes de acessá-lo, você deve fazer o log in no sistema de e-mail e para isto precisa de uma senha. Para não precisar ficar sempre lembrando e digitando a senha, você pode utilizar um software gerenciador de senhas, responsável por gerar e armazenar as mais diversas senhas, mas para acessá-lo você precisa de outra senha. Você coloca uma senha complexa neste software, mas precisará também de outra senha para acessar o computador para enviar o e-mail. Então resolve voltar atrás e deixar isso de lado e assinar digitalmente aquele e-mail sigiloso, mas lembra que também precisará de uma senha. Por fim, por mais forte que seja a criptografia utilizada, sempre haverá uma senha para protegê-la.

E já que precisamos de senhas, elas devem ser fortes. Para medir o quão forte uma senha é, devemos analisar, entre outras coisas, a quantidade total de senhas possíveis. Por exemplo, a senha de alguns cartões de crédito tem quatro números. Como são dez números possíveis, de 0 a 9, para calcular a quantidade total de senhas, devemos elevar este valor pelo tamanho da senha, desta forma estes cartões de créditos permitem 10^4 (10.000) possibilidades de senhas. Este é um número grande considerando que alguém venha a pegar seu cartão e tentar utilizá-lo, mesmo porque normalmente depois de três tentativas incorretas o cartão bloqueia. Entretanto, quando falamos de sistemas informatizados, o cenário muda. Em 2019 um computador tradicional consegue testar aproximadamente 16.036.446 senhas por segundo (BUYS, 2019) e além disto, vários sistemas não têm o controle de limite de senha incorreta.

Se você pesquisar na internet, há vários casos em que a Polícia Federal consegue quebrar a senha de algum acusado com seus supercomputadores, mas também há aqueles casos em que isso não foi possível, como foi o caso de um computador de um acusado da operação Lava Jato em 2018 (G1, 2017). Segundo a notícia: "Ganhar na Mega-Sena seria mais fácil". Isto tudo porque foi utilizada uma boa senha.

Existem vários programas utilizados para adivinhar ou quebrar senhas. Pesquise sobre o programa John the Ripper e se surpreenda como ele pode facilmente quebrar uma senha tradicional. QRCODE: <https://cartilha.cert.br/senhas/>.

Acesse o site e conheça algumas boas práticas para senhas recomendadas pela CERT.br (2018b).

Pesquise por "splashdata 100 worst passwords" e analise a pesquisa da SplashData, uma empresa de segurança da informação, com as 100 piores senhas do último ano. Se quiser, você também pode acessar: <https://www.teamsid.com/worst-passwords-2017-full-list/>. Acesso em: 26 abr. 2019.

Além das informações que você sabe, outra forma tradicional e antiga de fornecer o controle de acesso é com algo físico que você possui. Um grande e simples exemplo são as próprias chaves de portas. A seguir estudaremos mais sobre este mecanismo.

3.2 DISPOSITIVOS CRIPTOGRÁFICOS

Este mecanismo baseia-se em algo que o usuário possui e possa realizar a sua autenticação a partir de informações fornecidas por este objeto. Alguns exemplos são cartões magnéticos, chips, *smart cards* e *tokens* (GALVÃO, 2015).

Dentre as vantagens está o fato de que em alguns casos a duplicação do objeto pode ser mais cara do que o valor do que está sendo guardado e por poder armazenar senhas que a memória humana dificilmente conseguiria. As desvantagens aparecem por estes dispositivos poderem ser perdidos, roubados, esquecidos, inutilizados e por haver o custo adicional do hardware.

Como discutido na seção anterior, o elo mais fraco desta corrente está no armazenamento e proteção da senha e chaves criptográficas se estiver utilizando a criptografia. Então, como armazená-la de forma segura? A resposta é simples: utilizando dispositivos criptográficos. Eles são objetos que atestam informações acerca de uma entidade (pessoa física, jurídica ou ainda um equipamento), emitidos por uma terceira parte confiável entre todos que a aceitam. Um exemplo simples é seu cartão de crédito. Ele é algo físico que você possui, exige uma senha para ser utilizado, é emitido por alguém confiável como um banco e, em alguns casos, possui alguma informação biométrica sua.

Algumas características dos dispositivos criptográficos, e que atributos eles garantem segurança, são:

- Devem ser de difícil replicação (evitam clonagem).
- Devem identificar unicamente uma entidade (irretratabilidade).
- Devem tornar proibitiva a tentativa de adulteração (integridade).
- Devem conter um prazo de validade (temporalidade).
- Devem ter sido emitidos sob rigoroso processo de validação (autenticidade).

Temos dois exemplos principais de dispositivos criptográficos:

- *Smart cards* – idênticos aos cartões de crédito, com chip, utilizados atualmente, como o apresentado a seguir, da Certisign.

FIGURA 12 – SMART CARDS

FONTE: <https://www.certisign.com.br/certificado-digital/ecpf>. Acesso em: 24 abr. 2019.

- *Tokens* criptográficos – similares fisicamente a um simples pen drive, como o apresentado a seguir, da Certisign.

FIGURA 13 – TOKEN

FONTE: <https://www.certisign.com.br/certificado-digital/ecpf>. Acesso em: 24 abr. 2019.

O que estes dispositivos criptográficos têm em comum é que são dotados de capacidade computacional, possuem proteção contra tentativas de violação, gerenciam objetos (chaves, certificados digitais e senhas) e possuem duplo ou triplo fator de autenticação. Além disso, fornecem proteção às chaves privadas, utilizadas na criptografia. Uma vez geradas, estarão totalmente protegidas, não sendo possível exportá-las para uma outra mídia nem as retirar do dispositivo criptográfico.

Até aqui você já estudou os mais simples mecanismos, que são o que você sabe e o que você possui. Agora vamos aplicar um pouco mais de tecnologia através dos controles de acesso biométricos.

3.3 BIOMETRIA

Esse tipo de mecanismo de autenticação utiliza alguma característica física ou de comportamento do indivíduo. Os sistemas que utilizam a biometria trabalham com o conceito de verificação e identificação, comparando a característica biométrica lida com uma anteriormente armazenada no sistema (MORAES, 2010). Segundo Stallings (2015), a biometria pode ser classificada entre:

- Algo que o indivíduo é (biometria estática): como o reconhecimento por impressão digital, retina e face.
- Algo que o indivíduo faz (biometria dinâmica): como o padrão de voz, características de escrita manual e ritmo de digitação.

Como vantagem deste mecanismo de autenticação, tem-se que na maioria das biometrias não podem ser forjados, já que são únicas na natureza, não podem ser esquecidas e obriga que a pessoa a ser autenticada esteja fisicamente presente no momento da autenticação. Mas, como desvantagem, existe o alto custo de implementação, a aceitação pelos utilizadores e a falta de padrões em alguns sistemas.

Moraes (2010) apresenta o seguinte quadro comparando os principais sistemas biométricos. Cada um deles tem seus pontos fortes e pontos fracos, sendo indicados a uma ou outra aplicação.

QUADRO 1 – SISTEMAS BIOMÉTRICOS

Sistema Biométrico	Força	Fraqueza	Aplicação
Impressão digital	Estável ao longo do tempo	Resistência do usuário	Controle de acesso
	Única	Requer treino	Soluções de autenticação de aplicações
	Leitor pequeno e barato	3 a 7% da população não possui impressões legíveis ou estáveis	Caixas de bancos
			Veículos
Face	Não é intrusivo	Baixa precisão	Não é aceito em diversos países devido a leis de privacidade
	Não depende de participação do usuário	Pode ser enganado por foto	
		Usuário pode usar disfarce	
Face térmico	Muito preciso	Poucos produtos disponíveis	Não existe uso comercial ainda
	Não é enganado por foto		
Íris	Estável no tempo	Alta resistência	Acesso físico
	Alta precisão	Depende de treinamento com a câmera	Caixa de banco
			Passagem aérea
Geometria das mãos	*Template* pequeno	Tamanho do dispositivo	Ponto eletrônico
	Baixa taxa de erro na criação do *template*	Contato físico requerido	
	Não afetada pela condição da pele	O tamanho dos dedos de usuários jovens pode mudar	
	Não é intrusivo		
Retina	Estável no tempo	Requer treinamento do usuário	Controle de acesso
	Altíssima precisão	Alta resistência	
	Única	Tempo de leitura lento	
		Usuário não pode mexer a cabeça	
Voz	Facilidade de uso	A voz muda com o tempo e condições emocionais	Controle de acesso
	Baixo treinamento	Pouca precisão	Telefones celulares
	Não é intrusivo	Fácil de ser fraudado	Banco por telefone
	Pode ser usado para telefone		
Assinatura	Alta aceitação do usuário	Instável	Uso em dispositivos portáteis
	Mínimo treinamento	Muda com o tempo	Cartão de crédito
	Conveniente para transações financeiras	Requer várias leituras do usuário	

FONTE: Moraes (2010, p. 62)

RESUMO DO TÓPICO 2

Neste tópico, você aprendeu que:

- Os controles e medidas de segurança lógica são extremamente importantes, tendo em vista as diversas vulnerabilidades existentes.

- A criptografia pode e deve ser utilizada em vários níveis, para garantir a segurança da informação.

- As cifras de criptografia podem ser tão simples que uma criança pode utilizar, até o nível em que é necessário um supercomputador.

- Os mecanismos de autenticação podem ser algo que se sabe (como as senhas), que possui (como um cartão com chip), que se é (como a impressão digital) ou o que se faz (como o padrão de escrita).

AUTOATIVIDADE

Utilize o cenário do sistema para a Secretaria da Saúde, já apresentado na autoatividade anterior, para responder às questões a seguir.

1 (ENADE 2008 – Adaptado) Para elevar o nível de segurança do sistema da Secretaria da Saúde foi estabelecido que o acesso à interface web do servidor utilizará o protocolo HTTPS, onde uma sessão SSL é estabelecida entre browser do usuário e o servidor. Para tanto, usam-se mecanismos baseados em criptografia simétrica e assimétrica para prover serviços de segurança. Em comparação ao acesso HTTP, sem SSL, que serviços de segurança são providos para o usuário?

a) ( ) Autenticação do servidor e controle de acesso do cliente.
b) ( ) Autenticação do cliente e controle da velocidade de transmissão.
c) ( ) Autenticação da rede e proteção contra vírus.
d) ( ) Autenticação do servidor e confidencialidade das transmissões.

2 (ENADE 2011 – Adaptado) Para garantir o sigilo médico, foi estabelecido que a solução proposta deverá possibilitar uma forma de comunicação segura entre o médico e o paciente. Existe uma preocupação com a possibilidade de interceptação e alteração das mensagens durante as suas transmissões. Para reduzir a possibilidade de que um atacante tenha acesso ao conteúdo da mensagem, foi adotado um procedimento de criptografia de chave pública e assinatura digital. Considerando a utilização dessas tecnologias para a codificação da mensagem que será enviada do paciente (remetente) para o médico (destinatário), avalie as afirmações que se seguem:

I- Para o procedimento de cifragem da mensagem, é utilizada a chave pública do médico.
II- Para o procedimento de assinatura digital da mensagem, é utilizada a chave pública do médico.
III- Para o procedimento de decifragem da mensagem, é utilizada a chave privada do paciente.
IV- Para o procedimento de verificação da assinatura digital da mensagem, é utilizada a chave pública do paciente.

Assinale a alternativa CORRETA:
a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas I e IV estão corretas.
c) ( ) As afirmativas II e III estão corretas.
d) ( ) As afirmativas III e IV estão corretas.

3 (ENADE 2009 – Adaptado) Pesquisadores da área de tecnologia da informação advertem para o fato de que sistemas de informação computadorizados são mais vulneráveis a destruição, erros, mau uso e crime do que os sistemas manuais, em que a informação é geralmente guardada sob a forma de registros em papel. Analise as afirmativas a seguir, como formas possíveis de agregar segurança à solução que a Secretaria da Saúde está adotando.

I- Guardar todos os seus bancos de dados e seus respectivos backups utilizando as senhas padrões do sistema, que serão sempre seguras.
II- Instalar sistemas de segurança de acesso aos arquivos e sistemas, tais como log in e senhas.
III- Instalar sistemas de proteção contra vírus e hackers para poder se proteger contra-ataques internos e externos.
IV- Desativar o sistema de criptografia de dados para poder acelerar a velocidade de transmissão dos dados.

Assinale a alternativa CORRETA:
a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas I e IV estão corretas.
c) ( ) As afirmativas II e III estão corretas.
d) ( ) As afirmativas III e IV estão corretas.

4 (POSCOMP 2012 – Adaptado) Para aumentar a segurança no acesso às contas dos médicos no sistema da Secretaria de Saúde, solicitou-se que, além da biometria com impressão digital, fosse cadastrada uma senha composta por uma sequência de seis letras minúsculas. Nessas condições, e considerando o alfabeto com 26 letras, assinale a alternativa que apresenta, corretamente, a quantidade de possíveis senhas a serem formadas.

a) ( ) 81.092.624
b) ( ) 19.770.609.664
c) ( ) 165.765.600
d) ( ) 308.915.776

5 (LIQUIGAS 2012 – Adaptado) Os sistemas criptográficos contemporâneos se valem do poder de processamento dos computadores para criar algoritmos difíceis de quebrar, como os selecionados para a solução adotada pela Secretaria da Saúde. Essa mesma capacidade de processamento é uma das forças da criptoanálise. Nesse contexto, um dos conceitos (princípio de Kerckhoffs) que prevalecem para certificar ou homologar algoritmos criptográficos é que eles devem ser tão bem construídos que sua resistência a ataques de criptoanálise não deve residir no sigilo do algoritmo, mas, unicamente, no segredo da(o):

a) ( ) Chave.
b) ( ) Assinatura do remetente.
c) ( ) Identidade do destinatário.
d) ( ) Canal de transmissão.

6 (TCE-ES 2013 – Adaptado) Segurança se refere a algo que deve sempre estar em análise e evolução. Com o aumento do poder computacional, barreiras que antes tornavam o sistema seguro, agora não o fazem mais. Com referência ao controle de ativos de informação da Secretaria da Saúde, julgue os itens que se seguem e assinale a alternativa CORRETA:

a) ( ) O uso de biometria como mecanismo de autenticação do usuário no acesso aos sistemas de informação é cada dia mais utilizado e tem a vantagem de rápida implantação com baixo custo, possibilitando a instalação em todos os postos de saúde desta cidade.
b) ( ) Devido aos constantes ataques aos usuários de sistemas bancários, é cada vez mais comum a adoção de mecanismos de autenticação com base em segundo fator de autenticação. Seguindo este exemplo, poderia ser utilizada a senha e biometria para o acesso ao sistema da Secretaria de Saúde.
c) ( ) Para a segurança da informação, todas as informações são igualmente importantes. Deve garantir que, tanto as informações de salário dos funcionários, quanto os telefones de contato dos laboratórios, devem ser protegidas com o mesmo rigor.
d) ( ) Um dos controles de acesso aos sistemas de informação mais utilizados é a identificação pelo uso de log in do tipo usuário e senha. A vantagem nesse tipo de controle de acesso relaciona-se ao seu baixo custo e à possibilidade de se garantir o não repúdio no acesso, garantindo que o médico, paciente ou laboratório é quem ele diz ser.

7 (DATAPREV 2014 – Adaptado) Um tema muito recorrente, quando se pensa em segurança da informação, é a análise de riscos, que tem a função de indicar se um risco pode ou não ser aceito pela organização. Os riscos podem ser classificados como físicos, ambientais e riscos lógicos. Assinale a alternativa que contém o que pode ser considerado um risco lógico para este sistema da Secretaria da Saúde.

a) ( ) Cabo desconectado durante limpeza.
b) ( ) Vandalismo que gerou equipamentos destruídos.
c) ( ) Parada dos servidores por causa de um vazamento de água dentro do datacenter.
d) ( ) Ataque hacker.

SEGURANÇA FÍSICA E AMBIENTAL

1 INTRODUÇÃO

Para Schneier (2001, s.p.) "as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados". Com isto, devemos sempre tomar medidas de segurança em todas as frentes de ataque.

De forma similar ao tópico anterior, o objetivo deste tópico é identificar as ameaças, vulnerabilidades e medidas protetivas que podem ser utilizadas, agora para proteger física e ambientalmente os recursos da empresa, incluindo pessoas, dados, equipamentos, sistemas de suporte, mídias e suprimentos. Mais detalhes sobre a segurança física e ambiental serão apresentados na Unidade 3, na seção sobre as normas ISO/IEC 17799 e 27002.

> Vivemos em um mundo físico. Esse é um fato óbvio, mas é surpreendentemente fácil ignorá-lo quando discutimos a segurança da informação digital. Nossa tendência natural é considerar a segurança de computadores estritamente em um contexto digital, em que computadores são acessados apenas por meio de uma rede ou de uma interface digital bem especificada e nunca são acessados diretamente ou com ferramentas físicas, como um martelo, uma chave de fenda ou um frasco de nitrogênio líquido. Entretanto, no final, a informação digital deve residir fisicamente em algum lugar, como em estados de elétrons, meio magnético ou dispositivos óticos, e acessar essa informação requer o uso de uma interface entre os mundos físico e digital. Portanto a proteção de informação digital deve incluir métodos para proteger fisicamente essa interface (GOODRICH; TAMASSIA, 2013, p. 54)

2 SEGURANÇA FÍSICA

Para entender um pouco melhor o que é a segurança física, começamos com alguns exemplos do que ela inclui e que fazem parte do nosso cotidiano: cercas elétricas, grades nas janelas, guardas e seguranças no lado externo e interno do prédio, iluminação em todos os ambientes, chaves e fechaduras nas aberturas, crachás para funcionários, acompanhamento de visitantes, controles de propriedade e sistemas de detecção e monitoramento. Segundo Ferreira e Araújo (2008, p. 123):

> A segurança física desempenha um papel tão importante quanto à segurança lógica, porque é a base para a proteção de qualquer investimento feito por uma organização. Investir em diferentes aspectos da segurança sem observar suas devidas prioridades pode ocasionar uma perda de todos os recursos investidos em virtude de uma falha nos sistemas mais vulneráveis.

Devemos aplicar a segurança em todas as frentes. Lembre-se de que uma corrente é tão forte quanto seu elo mais fraco. Sobre estas frentes, de acordo com Foina (2009), os problemas mais comuns relacionados com a segurança física são:

- Roubo de insumos e de partes de computadores.
- Acesso de pessoas não autorizadas aos relatórios com dados estratégicos da empresa, ainda que dentro do setor de Tecnologia da Informação.
- Roubo de dados armazenados em arquivos magnéticos ou ópticos, com conteúdo de interesse da empresa (lista de clientes, arquivos de senhas etc.).
- Sabotagem em equipamentos e arquivos de dados.

Como exemplificado anteriormente, muitas das principais medidas preventivas de segurança física tratam do acesso indevido de pessoas não autorizadas a certas áreas da organização. Fontes (2006) cita três itens referentes ao acesso físico:

1- As áreas e os ambientes físicos da organização devem ter acesso restrito para visitantes e outras pessoas que não trabalham no local no dia a dia.
2- Os visitantes devem estar sempre acompanhados de alguém da organização.
3- Todas as pessoas no ambiente da organização devem estar identificadas com crachás e qualquer colaborador deve poder questionar pessoas sem identificação.

A segurança física deve providenciar mecanismos para restringir o acesso às áreas críticas da organização, desta forma, prevenindo o acesso físico não autorizado, danos e interferências com as instalações e informações da organização (ABNT, 2013). Isto normalmente é feito através da definição e utilização de perímetros de segurança e controles de acesso.

Estes perímetros de segurança funcionam como se fossem camadas de proteção, indo aumentando as restrições à medida que aumenta o valor do ativo protegido. Por exemplo, as proteções vão desde o controle de acesso ao prédio da organização, até sua sala de servidores e são aplicadas as mais diversas formas de garantia de segurança, desde uma catraca que necessita de uma autenticação para permitir a entrada, até mesmo uma sala cofre com isolamento total do mundo exterior cuja única forma de entrada de ar é enquanto a porta de acesso está aberta. Independentemente da forma como a proteção será feita, ela deve ser proporcional aos riscos identificados, por isso a necessidade de um bom estudo e planejamento de risco.

Sala cofre é um ambiente projetado para garantir a segurança física de equipamentos de hardware, formando uma sala dentro desta sala cofre. Ela tem a vantagem de ser um ambiente estanque, com proteção contra fogo, calor, umidade, gases corrosivos, fumaça, água, roubo, arrombamento, acesso indevido, sabotagem, impacto, pó, explosão, magnetismo e armas de fogo.

> Apesar de todos os cuidados em se definir os perímetros de segurança, essa ação não produzirá resultados positivos se os colaboradores não estiverem sintonizados com a cultura de segurança da informação. Essa cultura deve estar pulverizada em toda a organização e especialmente consolidada dentro das áreas críticas de segurança. A informação pertinente ao trabalho dentro dessas áreas deve estar restrita à própria área e somente durante a execução das atividades em que ela se torna necessária. Essas atividades sempre deverão ser realizadas sob supervisão para garantir a segurança. Quando houver atividade, essas áreas devem permanecer fechadas de forma validável, como, por exemplo, através do uso de lacres de segurança, e supervisionadas regularmente (CAMPOS, 2007, p. 169).

De forma complementar, para garantir uma proteção adequada para os ativos de informação importantes para o negócio, além das medidas de proteção das informações digitais e da sintonia com os colaboradores, as medidas de proteção devem levar em conta as questões relativas às informações armazenadas em meios não eletrônicos, ou seja, em meio físico, como aqueles impressos em papel. Para que os responsáveis pela preservação destes ativos possam planejar e implementar as medidas de proteção necessárias, devem ter uma noção clara de quais informações valiosas permanecem armazenadas fora dos meios eletrônicos, bem como dos fluxos por elas percorridos na organização (BEAL, 2008). Assim como os sistemas legados, as informações em meio físico também precisam de uma atenção especial, mas muitas vezes são desmerecidas.

Mesmo tomando todas as medidas preventivas de segurança lógica e física, ainda existe, por exemplo, a possibilidade de um curto circuito gerar um incêndio na sala do servidor e acabar gerando um impacto negativo gigantesco. Para cuidar desta e outras áreas, existe a segurança ambiental.

3 SEGURANÇA AMBIENTAL

Como já vimos nas seções anteriores, a segurança se subdivide, de forma simplificada, entre lógica, que trata das informações armazenadas em meio digital, e a física, que trata das informações armazenadas em meio físico e do acesso aos locais de armazenamento destas informações e das digitais. Um ponto que não é coberto

por estas áreas é a segurança relativa ao ambiente, como rede elétrica, energia alternativa e climatização, e contra causas naturais como enchentes, incêndios e deslizamentos de terra. Esta terceira área é chamada de segurança ambiental.

Sobre a segurança ambiental, de acordo com Beal (2008, p. 81), "a adequada proteção do ambiente e dos ativos físicos de informação, tanto como no caso do ambiente lógico, exige a combinação de medidas preventivas, detectáveis e reativas", como vimos no primeiro tópico. Ainda de acordo com Foina (2009, p. 184):

> Os cuidados a serem observados no projeto de uma instalação para Tecnologia de Informação são de ordem elétrica, ambiental (temperatura e umidade), segurança (física e patrimonial) e ergonômica. Portanto, é fundamental a organização desses recursos, para garantia da disponibilidade dos equipamentos, da segurança física e lógica, e da ergonomia dos equipamentos (facilidade de uso e garantia de boas condições de trabalho).

Não podemos esquecer que também é possível citar como ameaças para a segurança ambiental, além do já descrito, os incêndios, desabamentos, alagamentos, e problemas na rede elétrica (MEDEIROS, 2001). Alguns exemplos do que a segurança ambiental inclui são: proteção de energia, HVAC (*Healting, Ventilation and Air Conditioning* ou em português Aquecimento, Ventilação e Ar-Condicionado), proteção de água, detecção de fogo, combate ao fogo, evacuação, monitoramento e detecção ambiental.

Depois de introduzido os conceitos de segurança física e segurança ambiental, para exemplificar e aprofundar melhor o assunto, na próxima seção apresentamos um estudo de caso de um projeto de criação de um ambiente seguindo boas práticas de segurança física e ambiental.

4 ESTUDO DE CASO

Para exemplificar a importância, características e boas práticas da segurança física e ambiental, nesta seção abordaremos o exemplo do projeto de um local seguro para a instalação de uma infraestrutura de TI, baseado no material de TISAFE (2010). É importante salientar que os um bom projeto não deve se limitar aos itens aqui apresentados, pois este é somente um estudo de caso.

Abaixo você verá questões a serem consideradas como a defesa em camadas, a construção do edifício, o perímetro externo, a infraestrutura, o ambiente e também sobre as mídias físicas.

4.1 DEFESA EM CAMADAS

De acordo com Caruso e Steffen (1999), um ambiente de processamento de informações, como qualquer outra instalação sensível, deve ser localizado em uma área livre de quaisquer fatores de risco, exceto se a atividade da organização, por si só, envolver esses fatores. Nesse caso, se o ambiente de processamento de informações tiver que compartilhar a área com qualquer atividade de risco, as diretrizes de segurança devem ser aplicadas de maneira ainda mais estrita.

> O mais recomendável é a construção de um edifício exclusivo, localizado no centro de uma área exclusiva, acima do nível do solo, com as instalações sensíveis no centro do edifício e as áreas de apoio na periferia, seguindo o conceito das camadas concêntricas de segurança (CARUSO; STEFFEN, 1999, p. 210).

O maior objetivo da segurança física é integrar medidas de segurança para obter defesa em profundidade. Existem vários níveis de segurança, descrevendo um modelo de defesa em camadas, no qual o número de camadas de defesa vai depender da configuração da instalação e no qual os ativos mais valiosos devem ficar no centro do modelo de defesa.

Uma possível configuração destas camadas, buscando a defesa em profundidade, do mais externo para o mais interno, é a seguinte:

1- Terreno: muro com guarita e seguranças.
2- Prédio: paredes, cuja entrada possua catracas, seguranças e uma recepção.
3- Callcenter: portas de vidro com a necessidade de crachá para ter acesso.
4- Datacenter: portas de metal com a exigência de biometria para acesso.
5- Racks com chave e câmeras.
6- Sala cofre.

4.2 CONSTRUÇÃO

O primeiro ponto a ser considerado é a localização e o acesso, respondendo pelo menos às seguintes perguntas:

- Como é a criminalidade no local?
- Possui muito ou pouca visibilidade?
- Tem acessos de emergência?
- Historicamente sofreu danos com ameaças naturais?
- Como é o tráfego aéreo e terrestre no local?
- Tem estabilidade da rede elétrica?
- Possui proteção de perímetro como grades, cercas e portões?

Depois de encontrado o local, para a construção, devemos levar em consideração a localização das portas e janelas, das entradas do prédio utilizadas pelo público em geral, da área de recepção, das saídas de emergência, das escadas

e também do material empregado na construção, que deve ser adequado aos requisitos mínimos necessários definidos no projeto e em conformidade com o objetivo da instalação. Algumas questões a serem consideradas nas instalações físicas da sala de computadores e equipamentos são paredes e portas com resistência ao fogo, alarmes, monitoramento, fontes de água, distribuição de cabos e o acesso aos equipamentos.

4.3 PERÍMETRO EXTERNO

A segurança do perímetro da instalação deve possuir segurança também. A ISO 17799 (a ser detalhada na Unidade 3) utiliza a expressão perímetro de segurança, definindo-a como quaisquer elementos que estabeleçam uma barreira ao acesso indevido. Deve haver um acesso de veículos e outro acesso para pessoas, facilitando a segurança. Da mesma forma, deve haver estacionamento segregado de funcionários e visitantes. O espaço externo deve conter cercas, que detêm tentativas de invasão e complementam outros controles de acesso. Deve haver iluminação nas entradas, nos estacionamentos e em todas as áreas críticas para facilitar o controle, além de sistemas de detecção de perímetro. Deve possuir um circuito fechado de TV (CCTV – *Closed-circuit television*) e vigilância em pontos de controle de acesso, além de patrulhas em todo o perímetro.

Segundo Fontes (2006), todos os locais físicos em que se encontram recursos de informação devem possuir proteção de controle de acesso. Os pontos de controle de acesso são projetados para gerenciar o perímetro do ambiente e áreas abertas, o que inclui áreas de escape, estacionamentos, áreas de embarque e recebimento de mercadorias. Podem incluir guaritas, portões para controle de acesso de veículos, patrulhas de perímetros, estacionamentos de funcionários e visitantes, inspeções de veículos e monitoramento do CCTV. Muitas empresas terceirizam os guardas de segurança, o que pode criar vulnerabilidades na segurança física caso os funcionários externos não conheçam a política de segurança da empresa e, por isso, estes devem ser treinados.

4.4 INFRAESTRUTURA

Deve haver um sistema de suporte de infraestrutura de energia elétrica, HVAC, combate ao fogo, umidade e qualidade do ar. No quesito de energia elétrica, devem haver circuitos dedicados com acesso controlado aos painéis de distribuição de energia, transformadores e cabos de alimentação. Devem haver controles de desligamento de emergência, gravação de tensão e proteções contra falhas. Alguns exemplos de falhas são:

- blackout (falta de energia);
- período prolongado com tensão abaixo do normal;
- distribuição aleatória que interfere nos equipamentos;
- pequeno período de baixa tensão;

- alta tensão momentânea;
- alta tensão prolongada;
- ruído na linha/distúrbio em tensão normal.

Algumas fontes de backup de energia elétrica são os geradores de energia de emergência e os UPS (*Uninterruptible Power Supply*). E no caso de necessidade de utilização destes, as prioridades são iluminação, sistemas de controle de acesso físico, sistemas de proteção de arquivos, equipamentos de computação (mainframes, servidores e estações), equipamentos de comunicação, sistemas de telefonia e HVAC.

Sobre o cabeamento, ele pode ser feito por fibra ótica, fios de cobre ou por outros tipos existentes. A questão principal é que estes cabos devem ter a certificação necessária para o objetivo requerido e deve haver controle de acesso a armários e salas de passagem (*riser rooms*).

4.5 AMBIENTE

Nos requisitos ambientais, deve haver controle de umidade para evitar a corrosão dos equipamentos, o risco de eletricidade estática e o risco para conexões elétricas. Deve também haver controle da qualidade do ar, por exemplo: contra poeira; e proteção da água, por exemplo: com um sistema de detecção de misturas.

A respeito do fogo, duas grandes causas de incêndios em datacenters são: o sistema de distribuição de energia e os próprios equipamentos. A detecção de fogo pode ser feita de forma manual, ótica (que analisa se algo como a fumaça bloqueia a luz), pela temperatura e por ionização (reação a partículas carregadas na fumaça). Esses detectores podem ser colocados nos tetos, sobre tetos suspensos, dentro de pisos falsos e em dutos de ar. O combate ao fogo pode ser feito por extintores e por sistemas sprinklers.

Sprinkler é um componente do sistema de combate a incêndio que descarrega água quando for detectado um incêndio, por exemplo, quando uma temperatura predeterminada foi excedida. Ele é instalado ao longo do teto, interligados por tubos onde passarão água e sua função é reduzir ao mínimo os danos causados pelo fogo e pela água.

Sobre a infraestrutura para climatização, Caruso e Steffen (1999) citam três dicas importantes:

- Na implantação de uma instalação para ambientes de informações, o sistema central de condicionamento de ar é vital ao seu pleno funcionamento.
- Devido à necessidade do controle das condições ambientais e de confiabilidade para o sistema de condicionamento de ar, é recomendável a instalação de condicionadores do tipo compacto (self-contained) ou de central de água gelada.
- É conveniente que a água de condensação, gerada pelo sistema de climatização, seja canalizada diretamente para um dreno capaz de suportar o volume máximo de água condensada pelo ar-condicionado, com uma folga de pelo menos 50%.

4.6 MÍDIAS FÍSICAS

Outro item que também exigem atenção são as mídias. Elas podem estar armazenadas em salas especiais, armários e cofres, que podem estar dentro da empresa em um ambiente operacional ou fora da empresa e neste caso, deve possuir uma logística de transporte. Segundo Beal (2008), as mídias levadas para fora das instalações devem sujeitar-se a procedimentos de proteção e normas para que não permaneçam desprotegidas em áreas públicas.

Por fim, devemos lembrar que assim como em outras áreas da segurança da informação, educação, treinamento e conscientização são fundamentais. Isto é particularmente importante em empresas que incentivam o *home-office* com uso de equipamentos móveis.

LEITURA COMPLEMENTAR

O QUE VOCÊ ESTÁ FAZENDO COM OS SEUS DADOS?

Você já imaginou um mundo onde todas as suas preferências e gostos pudessem ser acessados por pessoas e empresas? Como seria se fosse possível saber os lugares onde vai, o que gosta de fazer, quem são seus amigos, onde são suas férias, qual seu restaurante preferido, quais os filmes, músicas e livros gosta, as pessoas que gosta (e as que não gosta), quais suas posições políticas, filosóficas e religiosas, sua orientação sexual, sua origem étnica e seu estado de saúde? Como você se sentiria se fosse possível descobrir novas coisas com base em todas essas informações, até coisas que você não saiba sobre você mesmo?

E se todas essas informações pudessem ser usadas contra você, para lhe discriminar indevidamente, oferecendo serviços ou produtos por um preço maior, retirando você de certos mercados, sendo usadas para tornar seu seguro, plano de saúde ou até mesmo o crédito mais caro? E se certos produtos e serviços nem fossem oferecidos para você, pois aparentemente não seriam para o seu perfil?

Como seria se o seu empregador baseasse oportunidades de promoções, ou mesmo sua despedida, com base nas informações que você deu em uma rede social e nem imaginava que poderiam ser usadas para essas finalidades? E se o seu perfil, derivado dessas informações anteriores, permitisse que você tivesse somente certos tipos de emprego e não outros?

O que poderia acontecer se os governos verificassem que a sua opinião sobre política não está alinhada com a posição dominante e usassem isso para lhe perseguir? Como você se sentiria se fossem mapeadas suas atividades mais básicas, como andar pela cidade, pegar um ônibus, táxi ou outros meios de transporte? Como você se sentiria se os governos soubessem todos os produtos que você compra e esses dados pudessem ser utilizados para atividades que você nem imagina? Como seria o mundo se todos pudessem ser facilmente identificados, mesmo à distância, com base em atributos pessoais, como formato do rosto e impressões digitais ou com base nas coisas que carrega? E se, mesmo sem que você queira, fosse possível descobrir todos os lugares em que você já foi, com quem você esteve e quais lugares você estará no futuro? E se além de governos, empresas também pudessem ter acesso a todas essas informações? E se não fosse necessária uma ordem judicial para autorizar alguém a ver tudo isso?

E se além das informações que você fornece voluntariamente, outras informações pudessem ser recolhidas, sem que você perceba, por coisas que você utiliza no dia a dia? Se o seu relógio, televisão, ar condicionado e geladeira estivessem recolhendo dados sobre o seu comportamento? E se a sua televisão pudesse "ouvir" e "ver" o que você fala diante dela e isso pudesse ser visto por outras pessoas? Como você se sentiria se as reações que você tem ao ver um comercial, ou filme, pudessem ser percebidas pela TV, indicando se você gostou ou não daquele conteúdo? E se todas essas coisas pudessem perceber quantas pessoas estão na sua casa, quem são e o que estão fazendo?

E se os carros pudessem ouvir o que as pessoas falam dentro deles? E se fosse possível criar um perfil seu com base nos lugares que vai de carro e, talvez, a velocidade média que dirige e frequência com que pisa no freio? E se informações indicassem que você pode não ser um bom motorista e isso fosse compartilhado com sua seguradora ou até mesmo o seu empregador? Ou ainda, se você nem conseguisse renovar o seu seguro em face dessas informações?

E se todos os produtos que você compra no supermercado fossem mapeados e pudessem ser utilizados para finalidades que você não previu? Como seria se o seu supermercado conseguisse prever o futuro, sabendo exatamente a data que você voltará lá?

Como seria se as preferências e as ações dos seus filhos pudessem ser mapeadas pelas empresas? E se as interações entre as crianças fossem registradas e fosse possível, desde muito cedo, prever padrões sobre o comportamento delas? E se o desempenho escolar e o comportamento das crianças pudesse ser medido por outras empresas, que não as escolas, e esses dados pudessem ser usados para discriminar as crianças (por exemplo, no futuro, por um empregador)? E se outras pessoas, além dos pais, também pudessem ter acesso a esses dados?

E se fosse possível criar um perfil seu, com base em todos os sites que você já visitou na vida, inclusive aqueles mais obscenos? Como seria se os programas que você usa no seu computador e os aplicativos do seu celular não se comportassem da forma como você espera e recolhessem informações suas sem que você perceba? E se todas as fotos tiradas com o seu celular, inclusive as mais íntimas, também pudessem ser vistas por empresas e outras pessoas? E se as câmeras de monitoramento residencial – inclusive aquelas utilizadas como babysitter cam – fossem acessadas sem autorização?

Como seria se os seus deslizes, gafes e erros (incluindo aqueles cometidos quando você era criança ou adolescente) pudessem ser registrados de alguma forma? E se esses dados, uma vez tornados públicos, perseguissem você sempre que se pesquisasse o seu nome na Internet?

E se o seu perfil, criado com base em todas essas informações anteriores, estivesse incorreto? Ou imagine que você nem soubesse quem tem acesso a quais informações suas e para que as utiliza. E como seria se você não conseguisse corrigir os erros desse seu perfil? Ou o que aconteceria se ele refletisse exatamente a sua personalidade, destacando, inclusive, seus piores defeitos? E se decisões sobre sua vida fossem tomadas, sem que você pudesse se opor – ou até mesmo saber – com base nessas informações? E se você não tivesse liberdade ou poder para controlar tudo isso?

O que aconteceria, por fim, se todos esses dados e todas essas informações sobre você, incluindo as incorretas, vazassem na Internet ou fossem mal utilizados por pessoas, empresas e governos? O que aconteceria se não houvesse leis para regular essas situações ou, se as que existem, não fossem suficientes?

Como você se sentiria se eu dissesse que isso tudo já estivesse acontecendo?

FONTE: GOULART, Guilherme Damasio. **O que você está fazendo com os seus dados?** 2017. Disponível em: https://www.segurancalegal.com/2017/01/artigo-o-que-voce-esta-fazendo-com-os-seus-dados/. Acesso em: 20 out. 2018.

RESUMO DO TÓPICO 3

Neste tópico, você aprendeu que:

- É importante entender os controles e medidas de segurança física e ambiental, tendo em vista as diversas vulnerabilidades existentes.
- Existem recomendações para a definição do espaço físico onde serão alocados os equipamentos contendo as informações.
- Os cuidados que devem ser despendidos sobre as mídias de armazenamento não podem ser menosprezados.
- A segurança ambiental, no que tange à rede elétrica, à energia alternativa, à climatização, entre outros fatores, devem ser levados em conta para o bom funcionamento dos equipamentos e consequentemente a segurança das informações.
- A segurança física deve ser planejada em um modelo de defesa em camadas que apresente uma variedade de medidas preventivas contra intervenções deliberadas e acidentais, bem como as ameaças ambientais.

Ficou alguma dúvida? Construímos uma trilha de aprendizagem pensando em facilitar sua compreensão. Acesse o QR Code, que levará ao AVA, e veja as novidades que preparamos para seu estudo.

AUTOATIVIDADE

Assim como feito nas autoatividades anteriores, utilize o cenário do sistema da Secretaria de Saúde para responder às questões a seguir, considerando as instalações onde os servidores deste sistema estão localizados.

1 (CESPE 2013 – Adaptado) Considere que o rompimento de um cabo tenha interrompido a comunicação entre uma das clínicas médicas e o servidor que provê o acesso ao sistema da Secretaria da Saúde, que utiliza cabeamento estruturado. Com base nisto, assinale a opção em que é apresentada uma área de segurança da informação segundo a qual os controles implementados podem prevenir esse tipo de incidente.

a) ( ) Segurança física.
b) ( ) Controle de acesso à rede.
c) ( ) Controle de acesso à aplicação e informação.
d) ( ) Segurança lógica.

2 (AGU 2014 – Adaptado) Segundo a Norma ISO/IEC 27002:2005, utilizada na preparação do prédio que hospeda o servidor, a segurança física e do ambiente tem como objetivo prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações. Considerando o que foi estudado até aqui, assinale a alternativa CORRETA acerca do perímetro de segurança física a ser seguido.

a) ( ) Devem-se construir barreiras lógicas e ambientais, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente.
b) ( ) As instalações de processamento da informação gerenciadas pela organização podem ficar fisicamente juntas daquelas que são gerenciadas por terceiros.
c) ( ) A localização e a capacidade de resistência de cada perímetro dependem dos requisitos de segurança dos ativos existentes no interior do perímetro, e dos resultados da análise/avaliação de riscos.
d) ( ) Os visitantes não precisam ser supervisionados, pois o registro da data e a hora da entrada e saída podem ser utilizados como o registro de acesso.

3 (TRE-MS 2012 – Adaptado) Uma das normas considerada na preparação do prédio do servidor é a ABNT NBR ISO/IEC 27.001. Dentre outras coisas, recomenta que a organização mantenha computadores desligados ou com a tela travada quando estes não estiverem em uso, além de não manter papéis com senhas ou descrição de acesso a informações críticas em locais desprotegidos, denominada "política de mesa limpa e tela protegida". Com base no que você estudou, a adoção desse tipo de política objetiva o controle de:

a) ( ) Gestão da continuidade do negócio.
b) ( ) Gestão de incidentes de segurança da informação.
c) ( ) Segurança de recursos humanos.
d) ( ) Acessos.

4 (CESPE 2016) Durante a preparação do prédio que hospeda o servidor do sistema da Secretaria da Saúde, foram levadas em consideração as principais normas de segurança lógica, física e ambiental. Para isto, várias medidas protetivas foram utilizadas. Correspondem a itens capazes de oferecer controle ou proteção no âmbito da segurança física preventiva.

a) ( ) As chaves públicas criptográficas.
b) ( ) Os dispositivos de autenticação biométrica.
c) ( ) Os sistemas de autenticação por senhas single sign-on.
d) ( ) Os certificados digitais.

5 (FCC 2018 – Adaptado) Depois de ataques sofridos, buscando definir a estrutura, as diretrizes e as obrigações referentes à segurança da informação para a solução da Secretaria da Saúde, foi definido uma política de segurança. Considere os seguintes controles da PS:

I- Controlar o acesso de pessoas às áreas em que se encontram os servidores computacionais.
II- Bloquear acesso dos funcionários para sites inseguros da internet.
III- Instalar firewall para controlar os acessos externos para a rede local da empresa.
IV- Controlar a temperatura das salas e corredores do prédio.

Os controles mencionados são, respectivamente, tipificados como de Segurança:

a) ( ) Física, Lógica, Lógica e Ambiental.
b) ( ) Física, Lógica, Física e Ambiental.
c) ( ) Lógica, Lógica, Ambiental e Lógica.
d) ( ) Ambiental, Física, Lógica e Física.

6 (FGV 2010 – Adaptado) No que diz respeito à segurança do ambiente do prédio que fornece a infraestrutura para o servidor da Secretaria da Saúde, vários são os pontos que foram considerados, como a climatização do local, às instalações elétricas e fonte de energia alternativa. A respeito da umidade, o verdadeiro efeito que a alta umidade do ar pode causar em equipamentos elétricos é:

a) ( ) O superaquecimento dos equipamentos.
b) ( ) A corrosão dos equipamentos.
c) ( ) O excesso de eletricidade dinâmica e a eventual queima de equipamento.
d) ( ) O aumento no consumo de energia para reduzir a temperatura.

UNIDADE 2

SEGURANÇA NO COTIDIANO

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- conhecer as principais características de segurança em um ambiente computacional e os principais motivadores de segurança;
- entender a importância dos controles e medidas de segurança física, lógica e ambiental, tendo em vista as diversas vulnerabilidades existentes;
- compreender os fatores de um sistema operacional que impactam na segurança da informação;
- saber sobre segurança da informação no contexto de redes de computadores.

PLANO DE ESTUDOS

Esta unidade está dividida em três tópicos. No decorrer da unidade você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – SEGURANÇA EM SISTEMA OPERACIONAL

TÓPICO 2 – OS PRINCIPAIS INVASORES

TÓPICO 3 – SEGURANÇA EM REDES DE COMPUTADORES

Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

TÓPICO 1

SEGURANÇA A NÍVEL DE SISTEMA OPERACIONAL

1 INTRODUÇÃO

Prezado acadêmico, durante a unidade anterior você aprendeu sobre o conceito de segurança da informação, propriedades de segurança da informação, riscos, ataques, criptografia, ameaças e vulnerabilidades. Tendo esse conhecimento consolidado, a partir de agora você estará apto a dar continuidade a seus estudos compreendendo como garantir a segurança da informação no seu cotidiano de trabalho.

Esta é a segunda unidade da disciplina de Segurança em Tecnologia da Informação, disciplina que objetiva proporcionar uma aprendizagem autônoma sobre os principais conceitos de segurança na área da tecnologia da informação, proporcionando a você o desenvolvimento de competências necessárias para a implementação da gestão da segurança da informação.

2 SISTEMAS OPERACIONAIS

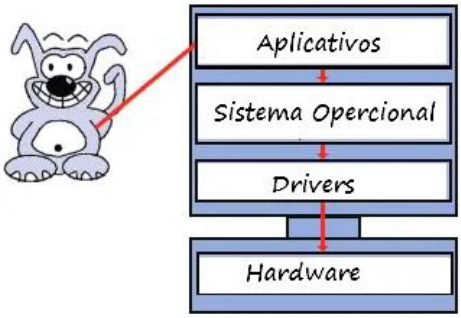
Daremos início aos nosso estudo conhecendo sobre as principais maneiras de proteger o sistema operacional. Todavia, primeiro, é importante relembrarmos o conceito de um sistema operacional.

De acordo com Tanenbaum e Bos (2016, p. 3), "os sistemas operacionais realizam duas funções essencialmente não relacionadas: fornecer a programadores de aplicativos (e programas aplicativos, claro) um conjunto de recursos abstratos limpo em vez de recursos confusos de hardware, e gerenciar esses recursos de hardware". De modo geral, sistemas operacionais contêm perspectivas:

- pela perspectiva do usuário ou programador (visão *top-down*): é uma abstração do hardware, fazendo o papel de intermediário entre o aplicativo (programa) e os componentes físicos do computador (hardware);
- ou numa visão *bottom-up*, de baixo para cima: é um gerenciador de recursos, controla quais aplicações (processos) podem ser executadas, quando e quais recursos (memória, disco, periféricos) podem ser utilizados.

De maneira simplificada, compreendemos um sistema operacional como um software que faz a interface entre os recursos de hardware, os aplicativos e você, como usuário. Compreender o que um sistema operacional faz, lhe tornará capaz de saber o quão importante é o papel de garantir a segurança em todo esse processo.

FIGURA 1 – SISTEMA OPERACIONAL



FONTE: <https://img-21.ccm2.net/2zNZYPvl4P0FujIR3JxgReFfuuE=/4751e80afd164787b1a36254735930d1/ccm-encyclopedia/0NbYFaM1-image-2-s-.png>. Acesso em: 5 dez. 2018.

Para trazer uma reflexão da importância de se garantir segurança da informação a nível de sistema operacional é importante conhecer algumas das inúmeras funções de um sistema operacional.

- Gestão do processador: o sistema operacional se encarrega de gerenciar o subsídio do processador entre os diversos programas, graças a um algoritmo de escalonamento. O tipo de programador é totalmente dependente do sistema operacional em função do objetivo visado.
- Gestão da memória RAM: o sistema operacional se encarrega de gerenciar o espaço de memória atribuído a cada aplicativo e, se for o caso, a cada usuário. No caso de insuficiência de memória física, o sistema operacional pode criar uma área de memória no disco rígido, chamada de memória virtual. Ela faz funcionar aplicativos que necessitam de mais memória do que a memória RAM tem disponível no sistema. Por outro lado, esta memória é muito mais lenta.
- Gestão das entradas/saídas: o sistema operacional unifica e controla o acesso dos programas aos recursos materiais através dos drivers (também chamados de gerenciadores de periféricos ou gerenciadores de entrada/saída).
- Gestão da execução dos aplicativos: o sistema operacional é responsável pela boa execução dos aplicativos, atribuindo-lhes os recursos necessários ao seu funcionamento. Desta maneira, ele também permite eliminar um aplicativo que não responda corretamente.
- Gestão dos direitos: o sistema operacional é responsável pela segurança ligada à execução dos programas, garantindo que os recursos sejam utilizados apenas pelos programas e usuários que possuam direitos para tanto.
- Gestão dos arquivos: o sistema operacional gerencia a leitura e a redação no sistema de arquivos e os direitos de acesso aos arquivos pelos usuários e aplicativos.
- Gestão das informações: o sistema operacional fornece diversos indicadores para diagnosticar o bom funcionamento da máquina.

FONTE: <https://br.ccm.net/contents/651-sistema-operacional>. Acesso em: 5 dez. 2018.

2.1 PARADIGMAS DE SEGURANÇA EM SISTEMA OPERACIONAL

Através dos paradigmas de segurança em sistemas operacionais, "as soluções de segurança geralmente utilizam o sistema de arquivos para armazenamento das senhas, embora criptografadas e acesso aos arquivos através de permissões" (MATTOS, 2004, p. 9). A segurança com foco em sistemas operacionais tem se tornado um importante item, pois impacta diretamente no usuário final. Kropiwiec e De Geus (2004) apresentam três paradigmas de segurança da informação em sistemas operacionais, são eles:

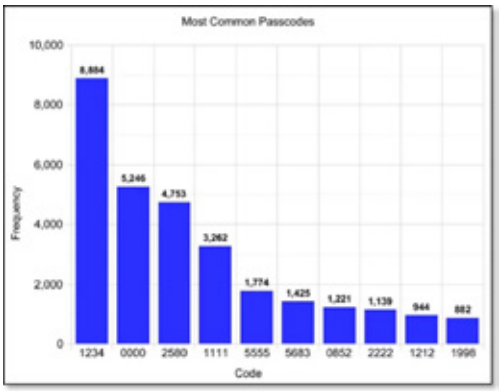
- **1º Paradigma - usuário limitador de segurança**: o usuário, ao criar arquivos e aplicações, aplica-se permissões de leitura e escrita, essas permissões são expandidas a um conjunto maior com ações mais específicas. O usuário poderá criar grupos de usuários que terão acesso a determinados arquivos, ficando a critério dele adicionar permissão ao grupo.
- **2º Paradigma - concentração e isolamento dos direitos privilegiados do computador**: os sistemas operacionais possuem um usuário, denominado superusuário (também chamado de administrador) que tem acesso a todos os recursos das máquinas, e ao qual são restritas todas as operações privilegiadas. É importante ressaltar que o administrador tem acesso irrestrito a todos os recursos do computador, inclusive os arquivos e aplicações pertencentes aos demais usuários. Os usuários comuns e suas respectivas aplicações só tem acesso ao que foi definido pelo administrador. Dessa forma, garante-se que os usuários não possam causar alguma falha de operação do sistema operacional, seja acidentalmente, seja intencionalmente.
- **3º Paradigma - cifragem de informações**: este paradigma tem uma forte relação com o conceito de criptografia, estudado na Unidade 1. São diversas as técnicas de cifragem, utilizadas para envio de arquivos pela rede e até mesmo para salvar arquivos em disco. Com a cifragem, o usuário tem a garantia de que, mesmo que alguém consiga acesso não-autorizado ao arquivo ou mensagem, esta será ilegível, sem a chave de criptografia apropriada. A única vulnerabilidade da cifragem é que o administrador poderá ter mecanismos de acesso ao arquivo criptografado.

2.2 SEGURANÇA EM SISTEMA OPERACIONAL

Quando o fator é segurança da informação em sistemas operacionais, não se limita a um único fator, a grande maioria deles dependerá do usuário. E a maior parte das vulnerabilidades acontecem por brechas que o usuário cria no uso do sistema.

Apenas no que se refere às senhas, são diversas as pesquisas que mostram que sequências, como 1234 ou repetições como 0000, são as senhas mais tradicionais utilizadas em dispositivos. Por uma outra perspectiva, há usuários que criam senhas complexas, que não guardam na memória, tornando necessário anotar em algum local.

GRÁFICO 1 – SENHAS MAIS COMUNS EM USUÁRIOS DE CELULAR



FONTE: <https://tecnoblog.net/wp-content/uploads/2011/06/senha-iphones.jpg>. Acesso em: 5 dez. 2018.

Um conceito que visa auxiliar a segurança a nível de sistema operacional foi discutido no Tópico 1: a criptografia, responsável por criar e utilizar mecanismos para que informações importantes não sejam conhecidas por quem não deve.

A única maneira segura de construir um sistema seguro é mantê-lo simples. Funcionalidades são o inimigo da segurança.

Para construir um sistema seguro, é preciso um modelo de segurança no núcleo do sistema operacional, simples o suficiente para que os projetistas possam realmente compreendê-lo, e resistir a todas as pressões para se desviar disso a fim de acrescentar novos recursos. Segundo Tanenbaum e Bos (2016):

- Base computacional confiável: são sistemas que têm exigências de segurança declaradas e atendem a essas exigências. No cerne de cada sistema confiável há uma TCB (*Trusted Computing Base* — Base Computacional Confiável) mínima consistindo no hardware e software necessários para fazer valer todas as regras de segurança (TANENBAUM; BOS, 2016, p. 416).
- Controle de Acesso a recursos: a segurança é muito mais fácil de atingir se há um modelo claro do que deve ser protegido e quem tem permissão para fazer o quê. Uma quantidade considerável de trabalho foi dedicada a essa área, então só poderemos arranhar a superfície nesse breve tratamento. Vamos nos concentrar em alguns modelos gerais e os mecanismos usados para serem cumpridos (TANENBAUM; BOS, 2016, p. 417).
- Modelos formais de sistemas seguros: essas seis primitivas podem ser combinadas em comandos de proteção. São esses comandos de proteção que os programas do usuário podem executar para mudar a matriz. Eles não podem executar as primitivas diretamente. Por exemplo, o sistema poderia ter um comando para criar um arquivo, que testaria para ver se o arquivo já existia e, se não existisse, criar um objeto e dar ao proprietário todos os direitos sobre ele. Poderia haver um comando também para permitir que o proprietário concedesse permissão para ler o arquivo para todos no sistema, na realidade, inserindo o direito de "ler" na entrada do novo arquivo em todos os domínios (TANENBAUM; BOS, 2016, p. 423).

Outro item que deve ser levado em consideração referente à segurança é a pluralidade de sistemas operacionais disponíveis. Há cerca de 10 anos, os profissionais de TI se preocupavam apenas com três sistemas operacionais (Windows, Linux e Mac), hoje se amplia com a ascensão dos smartphones e novos dispositivos como Raspberry pi e Arduino.

FIGURA 2 – PLURALIDADE DE DISPOSITIVOS

FONTE: <https://smallbiztrends.com/wp-content/uploads/2017/03/Too-Many-Devices-850x476.jpg>. Acesso em: 10 jun. 2019.

Windows perde o posto de sistema operacional mais usado do mundo

Uma pesquisa divulgada pela StatCounter mostra que o Android, sistema operacional do Google, ultrapassou no último mês de março o sistema da Microsoft em acessos à internet, com 37,93% de utilização, enquanto o Windows ficou com 37,91%. Os dados foram coletados de uma amostra que analisou a origem do tráfego de mais de três milhões de sites e páginas com mais de 15 bilhões de visualizações por mês. Essa é a primeira vez, desde os anos 80, que o Windows perde seu posto, de acordo com a pesquisar. O valor mostra o crescimento do Android, principalmente, em mercado asiático. "Na América do Norte, o Windows (todas as versões) manteve a liderança em todas as plataformas, com 39,5%, seguido pelo iOS (25,7%) e pelo Android (21,2%). O mesmo acontece na Europa, onde o Windows (51,7%) tem mais do que o dobro do Android (23,6%). No entanto, na Ásia, o Android tem 52,2%, bem mais do que os 29,2% do Windows", explica a empresa que realizou a pesquisa. Excluindo-se o tráfego de dispositivos móveis, no entanto, o sistema da Microsoft mantém a liderança, correspondendo a 84% dos dispositivos.

FONTE: <https://olhardigital.com.br/noticia/windows-perde-o-posto-de-sistema-operacional-mais-usado-do-mundo/67223>. Acesso em: 3 dez. 2019.

Os dados sobre número de sistemas operacionais deixam claro que, cada vez mais, temos uma diversidade de dispositivos e, respectivamente, de sistemas operacionais. A cada passo na evolução tecnológica é uma preocupação a mais com segurança. Temos que utilizar recursos e boas práticas que garantam desde a segurança da vovó que está utilizando seu smartphone até mesmo a de uma grande indústria que tem seus dispositivos conectados utilizando recursos de IoT.

Sendo assim, temos a difícil missão de responder a seguinte pergunta: como garantir a segurança a nível de sistema operacional?

A primeira resposta que vai resolver muitos problemas de segurança é: sempre utilize software original. Instalar um software sem licença é uma prática ilegal que, segundo a Lei n° 9.609/98, é cabível de seis meses a dois anos de prisão ou multa.

As empresas que desenvolvem sistemas operacionais têm todo um zelo com falhas de segurança e operativas, mantendo canais de comunicação com usuários e atualizações. Com isto, corrigem erros e falhas com frequência e atualizações são disponibilizadas, uma vez utilizando um software pirata não irá obter tais atualizações, comprometendo o sistema operacional.

Outro risco que você corre ao instalar um software pirata é o dele não ser o real software que você requisitou. Ou seja, você pode ter realizado o download de uma outra aplicação maliciosa que colete seus dados e utilize-os para fins maldosos.

FIGURA – CHARGE: VIDA DE PROGRAMADOR

FONTE: <https://vidadeprogramador.com.br/wp-content/uploads/2011/04/tirinha71.png>. Acesso em: 10 dez. 2018.

Tendo como objetivo aumentar a segurança da informação, algumas boas práticas são recomendadas. Uma vez que qualquer vulnerabilidade no sistema operacional pode comprometer a segurança dos dados e aplicativos armazenados. No que se refere às boas práticas para garantir a segurança a nível de sistema operacional, a IBM (TÉCNICAS, 2017) recomenda as seguintes práticas de segurança:

- Contas do usuário: recomenda-se limitar o número de contas do usuário nos computadores servidores. As contas de usuário desnecessárias e legadas aumentam a complexidade do sistema e podem apresentar as vulnerabilidades do sistema. Ao deixar um número menor de contas de usuário reduz a quantidade de tempo que os administradores gastam na administração de contas. Deve se assegurar que poucos usuários confiáveis tenham acesso administrativo aos computadores servidores. Um número menor de administradores facilita a manutenção da prestação de contas, bem como garantindo que os administradores devem ser competentes. Designe o mínimo de permissões de acesso necessárias para a conta que executa o aplicativo. Se os invasores obtiverem acesso ao aplicativo, eles terão permissões do usuário que executa o aplicativo.
- Políticas de conta: desenvolva e administre políticas de senha que promovam a segurança do sistema operacional. Exemplos dessas políticas são a regra de senha forte e o planejamento de mudança de senha (a cada 15 dias, por exemplo). Teste a força das senhas do usuário quebrando-as (por exemplo, obrigar usuários a utilizarem caracteres especiais e números. Em sistemas operacionais UNIX/LINUX, as senhas são armazenadas no arquivo /etc/passwd. Este arquivo é aberto para todos, o que apresenta um risco de segurança. Para aprimorar a segurança da senha, ative o arquivo de senha sombra, denominado /etc/shadow. Se este arquivo estiver disponível, as senhas serão armazenadas nele ao invés do arquivo de senha. Como as permissões para o arquivo /etc/shadow são mais restritivas, o risco de segurança é menor. Um ponto importante no gerenciamento de contas é o conceito de *default deny* (negar por padrão), ou seja, por padrão, negar acesso a todos os usuários.
- Sistema de arquivos: os sistemas de arquivos são a maneira com que seu sistema operacional gerencia todo armazenamento em disco. Conceda aos usuários permissões somente de leitura para os diretórios necessários. Se os invasores obtiverem acesso a um aplicativo, eles terão permissões do usuário. É possível negar permissões de leitura e gravação para todas as estruturas de diretório para todos os usuários. Apenas os usuários – os quais essas permissões são concedidas explicitamente – têm acesso aos diretórios e aos arquivos. Essa política também protege todos os recursos que foram negligenciados por um administrador.
- Serviços de rede: nós teremos um momento para abordar, especificamente, segurança da informação voltada para redes de computadores, todavia, este tópico é destinado ao que fazer a nível de sistema operacional para garantir segurança em serviços de rede. Nesse quesito, é recomendável fornecer o número mínimo de serviços de rede necessários no computador servidor. Utilizando, assim, apenas os serviços necessários para executar o aplicativo. Cada serviço de rede é um potencial ponto de entrada para ataques maliciosos. A redução do número de serviços em execução também torna seu sistema

mais gerenciável, por exemplo, talvez você não precise de serviços de acesso remoto, então pode removê-los ou desativá-los, deixando menos maneiras de ter o acesso ao dispositivo por terceiros. Reduza o nível de permissões de acesso para os usuários de serviços de rede. Assegure-se de que as contas de usuário, que têm acesso ao servidor da web, não tenham acesso às funções *shell*. É importante garantir que serviços não utilizados não estejam em execução e, principalmente, de que não sejam iniciados automaticamente em sistemas operacionais, principalmente no Microsoft Windows, no qual isso é comum de acontecer. Finalizando, mas, não descartando sua importância, para garantir segurança nos serviços de rede é manter sempre o firewall ativado e atualizado de acordo com orientações do fabricante.

- Correções do sistema: execute as correções mais recentes recomendadas pelo fornecedor para o sistema operacional, tais correções são realizadas com as atualizações do sistema. As correções podem ser correções principais do sistema operacional ou requeridas por aplicativos adicionais. Planeje a manutenção regular das correções de segurança.
- Minimização de sistema operacional: remova aplicativos não essenciais para reduzir possíveis vulnerabilidades do sistema. Restrinja os serviços locais aos serviços necessários para operação. Implemente proteção para estouro de *buffer*. Você pode precisar de um software de terceiros para isso.
- Criação de log e monitoramento: registre eventos relacionados à segurança, incluindo log ons e log offs com êxito e com falha, e mudanças nas permissões do usuário, uma vez criados é importante monitorá-los.

3 O QUE É FIREWALL? QUAL SUA IMPORTÂNCIA PARA A SEGURANÇA DO SISTEMA OPERACIONAL?

O *Firewall* é um importante mecanismo, tem como principal objetivo restringir acesso ao seu dispositivo via rede. Existem tanto proteções de *firewall* a nível de software, quanto de hardware. Em um ambiente de sistemas operacionais o termo *firewall* é muito comum, bem como no universo de segurança da informação.

FIGURA 3 – FIREWALL PAREDE DE FOGO

FONTE: <https://www.estudopratico.com.br/wp-content/uploads/2015/08/firewall.png>. Acesso em: 14 jun. 2019.

O termo *firewall* é uma analogia à barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo. Em inglês, *firewall* é o nome dado às portas antichamas utilizadas nas passagens para as escadarias em edifícios. Em segurança da informação, os *firewalls* são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede, mas também a confidencialidade deles. Os softwares com a função de *firewall* já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez (SOUZA; SOUSA, 2010).

O *firewall* é uma parte essencial de configuração de segurança, pois serve como uma camada extra de proteção, mesmo que os serviços implementem funcionalidades de segurança por si mesmos, restringindo acesso a tudo, exceto aos serviços que necessitam ser mantidos abertos, essa medida reduz a superfície de ataque ao servidor, limitando os componentes que são vulneráveis à exploração.

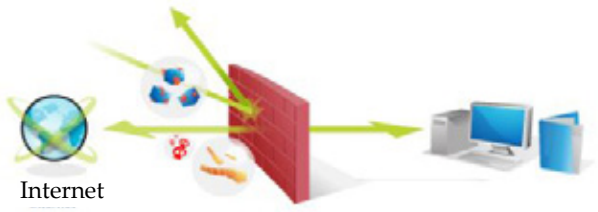
Segundo Kurose (2013 *apud* AZEVEDO; RIBEIRO, 2019, p. 27) um *firewall* possui três objetivos principais:

> 1- Obrigar que todo o tráfego de uma rede, com destino diferente de sua origem, passe por um *firewall*. Muito embora algumas organizações implementem *firewall* de vários níveis, a arquitetura mais comum consiste em sua alocação em um único ponto de entrada da rede.
> 2- Controlar a rede de modo que apenas o tráfego de pacotes autorizados aconteça.
> 3- Ser imune à penetração. Como se trata do principal ativo de segurança de rede um *Firewall* vulnerável se torna uma ameaça gravíssima a rede como um todo

No que se refere ao *Firewall* em forma de softwares:

> Aplicações com a função de *firewall* já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez. Os *firewalls* trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino (MACHADO, 2012, p2)

FIGURA 4 – *FIREWALL* DE SOFTWARE



FONTE: <http://www.milesweb.com/blog/wp-content/uploads/2012/07/Home-Networking16.png>. Acesso em: 15 dez. 2018.

Na forma de hardware, trata-se de equipamentos que são especificamente desenvolvidos e utilizados com a finalidade de proteção, e, normalmente, também são utilizados em aplicações empresariais. Segundo Petrin (2015, s.p.):

> O hardware, ao invés de ser dividido com várias funções como o software da máquina, é usado exclusivamente para isso, tratamento mais requisições e aplicando de forma mais ágil todos os filtros necessários para que a proteção seja feita da melhor forma. Alguns roteadores de rede domiciliar, inclusive, nos dias de hoje, contam com aplicações *firewall*, sendo que a mais básica se refere ao controle dos computadores que podem conectar-se à internet.

FIGURA 5 – EQUIPAMENTO *FIREWALL*

FONTE: <http://twixar.me/hpdT>. Acesso em: 5 jun. 2019.

RESUMO DO TÓPICO 1

Neste tópico, você aprendeu que:

- Os sistemas operacionais realizam duas funções essencialmente não relacionadas: fornecer a programadores de aplicativos (e programas aplicativos, claro) um conjunto de recursos abstratos limpo em vez de recursos confusos de hardware, e gerenciar esses recursos de hardware

- Através dos paradigmas de segurança em sistemas operacionais, as soluções de segurança geralmente utilizam o sistema de arquivos para armazenamento das senhas, embora criptografadas e acesso aos arquivos através de permissões.

- Ao criar arquivos e aplicações, aplica-se permissões de leitura e escrita, essas permissões são expandidas a um conjunto maior com ações mais específicas.

- Os sistemas operacionais possuem um usuário, denominado superusuário (também chamado de administrador) que tem acesso a todos os recursos das máquinas, e ao qual são restritas todas as operações privilegiadas.

- Com a cifragem, o usuário tem a garantia de que, mesmo que alguém consiga acesso não-autorizado ao arquivo ou mensagem, esta será ilegível, sem a chave de criptografia apropriada. A única vulnerabilidade da cifragem é que o administrador poderá ter mecanismos de acesso ao arquivo criptografado.

- A única maneira segura de construir um sistema seguro é mantê-lo simples. Funcionalidades são o inimigo da segurança.

- O *Firewall* é um importante mecanismo, tem como principal objetivo restringir acesso ao seu dispositivo via rede.

- O termo *firewall* é uma analogia à barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo.

- O *firewall* é uma parte essencial de configuração de segurança, pois serve como uma camada extra de proteção, mesmo que os serviços implementem funcionalidades de segurança por si mesmos, restringindo acesso a tudo, exceto aos serviços que necessitam ser mantidos abertos.

AUTOATIVIDADE

1 Garantir a segurança em sistema operacional se torna um desafio para usuários e profissionais de tecnologia, dentre tais mecanismos existem os paradigmas de segurança da informação. Selecione a alternativa CORRETA que contenha os paradigmas.

a) ( ) Usuário garantidor de segurança; concentração e isolamento dos direitos privilegiados do computador; Liberação de Informações.
b) ( ) Usuário limitador de segurança; concentração e isolamento dos direitos privilegiados do computador; cifragem de informações.
c) ( ) Computador limitador de segurança; coação dos direitos privilegiados do computador; cifragem de informações.
d) ( ) Chave restritiva de segurança; dispersão e inclusão dos direitos privilegiados do computador; decifragem de informações.

2 A segurança em sistemas operacionais remete ao emprego de várias estratégias. Sobre serviços de rede em sistemas operacionais assinale a alternativa CORRETA.

a) ( ) Neste quesito não é recomendável fornecer o número mínimo de serviços de rede necessários no computador servidor. Sendo assim, não há como garantir segurança a nível de rede em sistemas operacionais.
b) ( ) Neste quesito é recomendável fornecer o número máximo de serviços de rede necessários no computador servidor. A melhor saída é sempre fornecer o máximo de acesso possível.
c) ( ) Neste quesito não é recomendável fornecer o número mínimo de serviços de rede necessários no computador servidor. Para evitar riscos de segurança em sistema operacionais, o ideal é desabilitar tais recursos.
d) ( ) Neste quesito é recomendável fornecer o número mínimo de serviços de rede necessários no computador servidor. Utilizando, assim, apenas os serviços necessários para executar o aplicativo. Cada serviço de rede é um potencial ponto de entrada para ataques maliciosos.

3 Os sistemas operacionais são interfaces que permitem aos usuários interagir com o computador sem que seja necessário saber "falar a língua" dele. Sobre segurança em sistemas operacionais assinale a alternativa CORRETA.

a) ( ) Em sistemas operacionais Linux não há risco e nem vulnerabilidades.
b) ( ) Atualizar o sistema operacional é recomendado, pois previne contra falhas que foram corrigidas.
c) ( ) Para evitar riscos de segurança em sistema operacionais, o ideal é formatar o computador com frequência.
d) ( ) Para garantir segurança em sistemas operacionais o ideal é sempre utilizar sistema operacional MacOS.

4 O sistema operacional é o ambiente físico onde seu aplicativo é executado. Qualquer vulnerabilidade no sistema operacional pode comprometer a segurança do aplicativo. Selecione a alternativa CORRETA sobre boas práticas de segurança em sistemas operacionais.

a) ( ) Não instalar softwares ditos “piratas” é uma boa prática que visa garantir a segurança em sistemas operacionais.
b) ( ) Não atualizar o sistema operacional é recomendado, pois previne contra falhas que foram corrigidas.
c) ( ) Para evitar riscos de segurança em sistema operacionais, o ideal é formatar o computador com frequência.
d) ( ) Para garantir segurança em sistemas operacionais o ideal é sempre utilizar sistema operacional on-line.

5 O sistema operacional é o conjunto de programas que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída e dados da máquina e seus periféricos. O firewall exerce um importante papel para auxiliar na segurança a nível de sistema operacional.

Sobre firewall, assinale a alternativa CORRETA:
a) ( ) Os firewalls são os programas invasores, utilizados para roubar dados dos usuários.
b) ( ) Os firewalls são os programas antivírus.
c) ( ) Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino.
d) ( ) Os firewalls são os usuários na internet que trabalham para garantir a segurança dos dados.

OS PRINCIPAIS INVASORES

1 INTRODUÇÃO

Na última seção, vimos como é importante nos resguardar com relação à segurança em sistemas operacionais, revendo conceitos essenciais das funcionalidades e entendendo como tais sistemas podem estar vulneráveis. Um destaque especial à importância de sempre manter o sistema atualizado e deixar o mínimo de espaços para invasores.

Assumindo que, até aqui, você já garantiu todos os recursos de segurança a nível de sistemas operacionais através de boas práticas. A partir de agora, vamos começar a tratar de itens que vão além da capacidade do sistema operacional, dando continuidade pela perspectiva do software.

2 SEGURANÇA PELO SOFTWARE

A segurança é um atributo do sistema que reflete sua capacidade de se proteger de ataques externos, sejam acidentais ou deliberados. Esses ataques são possíveis, pois a maioria dos computadores de uso geral recebe informações de mecanismos externos, seja um dispositivo de dados (pen drive) ou via conexão de rede.

O grande ponto é que poderíamos utilizar um livro inteiro para tratar de segurança a nível de desenvolvimento de aplicações, desde boas práticas até recursos mais avançados. No entanto, vamos estudar alguns itens que irão auxiliar-nos de modo geral a garantir a segurança com a utilização de softwares, bem como compreender quais são as ameaças nesse nível.

Entrando na temática software, a partir do próximo subtópico iremos conhecer os principais tipos de softwares com o objetivo de explorar vulnerabilidades e atacar a segurança da informação.

3 MALWARES: OS SOFTWARES MALICIOSOS

Se você já passou por algum susto com invasão no seu computador, é possível que já tenha tido um primeiro contato com esse tipo de software, que sorrateiramente invadem o computador e causam algum dano.

Os Malwares (*Malicious* softwares) assim como diz sua tradução, são softwares maliciosos, que, independente da maneira com que chegaram ao seu dispositivo, com certeza não tem boa intenção.

De acordo com a *Cartilha de segurança para internet* (CERT.BR, 2017), os Malwares são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela autoexecução de mídias removíveis infectadas, como pen drives;
- pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Quando esses programas passam a estar no disco, seja por cópia magnética ou baixados da Web, geralmente são executados automaticamente dando acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

A charge a seguir ilustra um caso muito comum hoje em dia: como as empresas conseguem seu telefone? A resposta pode ser um malware, que invadiu seu dispositivo e compartilhou seu número.

O exemplo do telefone pode ser considerado simplista, tendo em vista que hoje pessoas tem informações de gestão, documentos pessoais e, principalmente, acessos financeiros em seus dispositivos. Um ataque de malware poderia obter e espalhar essas informações.

FIGURA 6 – COMO PLUGINS "MALIGNOS" E MALWARES ROUBAM SUAS INFORMAÇÕES?

FONTE: <www.pcfaster.com/en/computer-knowledge/How-malicious-plugins-malware-steal-your-information.html>. Acesso em: 2 dez. 2018.

Veremos, na sequência, os principais tipos de malwares acompanhados das maneiras de prevenção e combate.

3.1 VÍRUS

Começamos pelo mais famoso, ainda que nem sempre seja o grande vilão, geralmente independente do malware que o usuário esteja enfrentando ele irá chamar de vírus.

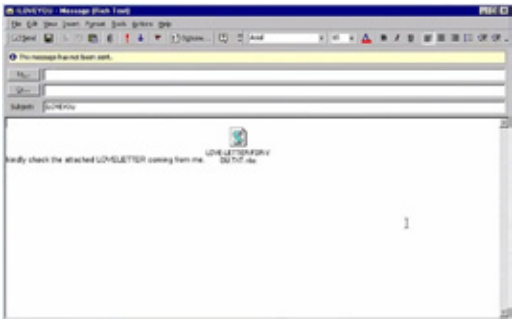
O nome vírus se dá principalmente pelo fato de se propagar rapidamente, assim como os vírus biológicos. Este tipo de malware infecta o dispositivo que foi instalado, realiza sua funcionalidade (apaga arquivos, rouba dados etc.) e depois utiliza-se dos recursos dos dispositivos para se propagar para os demais dispositivos.

Geralmente os vírus são danosos, ou seja, causam algum dano ao sistema. Estes danos podem ser a remoção ou alteração de arquivos importantes do sistema, mas existem vírus mais zombeteiros que trocam ícones, transformam pastas em atalhos, entre outras brincadeiras de mau tom.

Antes que você pense que os vírus são apenas criados de brincadeirinha por programadores que estão com tempo de ócio e que isso nunca irá lhe gerar prejuízo. Vale a pena lembrar o famoso caso de um vírus chamado *I love you* (eu te amo), se considerado o número de usuários da época, foi disparado para o mundo inteiro. O fato aconteceu no ano 2000, atingindo e destruindo arquivos de mais de 50 milhões de usuários, o vírus também impediu que PCs fossem inicializados, copiou senhas das pessoas e as repassou aos seus criadores, sendo estimado um prejuízo de mais de US$9 bilhões.

A Figura 7 mostra a tela de recebimento do vírus *I love you*, o que mais chama atenção é o anexo do e-mail, um arquivo com a extensão *VBS* (*Visual Basic Script*), uma linguagem de programação executada em aplicações Microsoft Windows. E-mails com este tipo de extensão se tornaram comuns em envios com intenção maliciosa, por isso os serviços de e-mail bloqueiam seu envio, e, em caso de recebimento, irão alertar os usuários sobre os perigos.

FIGURA 7 – O VÍRUS *I LOVE YOU*



FONTE: <https://vignette.wikia.nocookie.net/malware/images/3/3a/LoveAttach.jpg/revision/latest/scale-to-width-down/310?cb=20140512030813>. Acesso em: 3 dez. 2018.

Muito do que veremos aqui poderá ser útil na prevenção de demais malwares. Afinal, é isso mesmo, a maior defesa contra os vírus é a PREVENÇÃO. Por isso seguem algumas dicas:

- Tenha sempre um software antivírus instalado.
- Mantenha seu antivírus sempre atualizado.
- Cuidado com remetentes desconhecidos, nunca faça download, nem clique em links de estranhos.
- Atente-se às extensões, os vírus comumente vêm em formatos .exe, no entanto há diversas maneiras de serem ocultados.
- Cuidado com o armazenamento de dados pessoais, opte por serviços que garantam a segurança no armazenamento na nuvem, evite ao máximo informá-los via e-mail.
- Crie senhas intercalando letras, números e símbolos, criando uma senha para cada recurso que utiliza.
- Evite utilizar aplicativos de download do tipo torrent, P2P e Magnet Link, você nunca sabe a fonte que está te enviando.
- Atente-se aos dispositivos que se conecta, sejam smartphones, HDs externos, pen drives, os vírus mais antigos, e que mais se transmite, são via meio magnético.
- Ao instalar um programa sempre realize o download do site do fabricante e não de terceiros.

Se você assistiu à sequência de filmes do Indiana Jones, de primeira mão irá compreender a referência da charge a seguir com o que acontece diariamente na Web em relação ao filme. Muitas vezes, quando usuários acessam sites que não são confiáveis, acessam mais propagandas – porta para malwares – do que o real conteúdo que estão buscando. Lembrando que os sites de conteúdo pirata são os campeões quando se trata deste quesito.

FIGURA - O CAVALEIRO E AS ESCOLHAS DO DOWNLOAD

"Você deve clicar, mas clique sabiamente.
Porque, como o verdadeiro botão lhe trará o arquivo,
o falso botão derreterá seu rosto"

FONTE: <https://br.pinterest.com/pin/825003225464673822/>. Acesso em: 3 dez. 2018.

Agora que você já conhece o conceito do que é um vírus, e algumas maneira de preveni-los que podem ser úteis em diversos cenários, nos próximos subtópicos vamos conhecer outros tipos de malwares.

Vírus de Pen Drive - Uma praga que assombra as corporações a mais de 10 anos

Seguinte situação provavelmente é familiar: você vai usar seu pen drive e ele começa a esconder seus arquivos com atalhos. Faz uma pesquisa rápida na internet, e descobre que pegou um VÍRUS! A partir daí você se esforça para se lembrar dos locais em que o usou recentemente – no trabalho, em um computador público ou na casa de um amigo –, tentando adivinhar onde o dispositivo foi infectado. Mas a verdade é que qualquer desses lugares pode ter sido o culpado. E felizmente, por mais que sejam várias as possibilidades de tipos de vírus, não costuma ser difícil se livrar deles!

Pela forma como agem já dá para saber bem como resolver o problema.

Quer aprender a remover vírus do pen drive?

Então veja as nossas dicas a seguir e garanta a segurança dos seus arquivos e do seu computador.

Saiba como remover o vírus de um pen drive

Antes de mais nada, você pode poupar muita dor de cabeça simplesmente contando com o poder de um antivírus para resolver seu problema. Em certos casos, esse recurso é perfeitamente capaz de limpar seu pen drive das ameaças e recuperar seus arquivos sem maiores estragos.

As versões mais recentes do Windows – como o 8 e o 10 – possuem um antivírus nativo que realiza verificações bastante competentes a respeito da integridade das pastas e dos arquivos. Para isso, basta acessar o Windows Defender e realizar uma verificação apenas no seu pen drive. Após essa análise, o problema será diagnosticado e uma solução devidamente oferecida.

Conforme vamos confiando cada vez mais partes do nosso trabalho aos computadores, torna-se cada vez mais importante cuidarmos da segurança e da integridade dos nossos dispositivos. Então mantenha seu pen drive livre de vírus e conte sempre com seus arquivos acessíveis!

FONTE: <https://www.meliuz.com.br/blog/remover-virus-pen-drive/>. Acesso em: 4 dez. 2018.

3.2 SPYWARE

O spyware é um tipo de malware denominado espião e ao contrário dos vírus não realizam nenhuma ação de danificação, e por serem programas espiões, são dificilmente detectados. Como seu nome diz, sua função é espionar, ou seja, ele é instalado no dispositivo monitorando o usuário e coletando as informações, que são enviadas para seus criadores. Há duas divisões com relação à maneira com que os spywares são obtidos e instalados:

- Spyware legítimo: é um software que o próprio usuário instala em sua máquina com o objetivo de monitorar a atividade de outros usuários. Tem se tornado uma prática comum em empresas com a finalidade de monitorar os funcionários. Tal prática tem se tornado alvo de debates por profissionais e juristas.
- Spyware malicioso: este é o caso que temos de combater, pois é quando o spyware tem a forma de um malware e é instalado no computador sem a autorização do usuário.

Com os avanços da Web cada vez mais se evoluem os spywares maliciosos, que podem ser divididos em três tipos principais:

- KeyLoger: é instalado com objetivo de capturar o que o usuário está digitando. O objetivo deste tipo de aplicação é obter as senhas dos usuários, principalmente de serviços que envolvam transações financeiras como sites de banco.
- Screenlogger: funciona como se apertasse a tela de PrintScreen a cada clique do mouse. Tem os mesmos objetivos que o keyloger, no entanto, com foco em teclados virtuais (que deveriam ser dispositivos de segurança.
- Adware: é o típico programa que invade sua máquina para encher seu navegador e aplicativos de propaganda ou até mesmo alterar endereços como a página inicial. Existem muitos com fins legítimos, ou seja, direcionam para sites reais, o que não significa ser uma prática legal.

3.3 TROJANS HORSES

Os *trojan horses*, ou apenas trojans, são programas de computadores denominados cavalos de Tróia, que seguem a ideia da história real. São programas de computador que realizam a função para a qual foram designados e mais alguma função maliciosa.

3.4 ROOTKIT

Não é exatamente um programa e se não fosse uma técnica maliciosa poderíamos dizer se tratar de um conjunto de boas práticas, mas são um conjunto de práticas maliciosas que garantem que a presença de um invasor não seja notada em um dispositivo.

Tais conjuntos são utilizados para remover os rastros dos invasores, tentar ocultar a presença do antivírus e do firewall, bem como impedir que algum especialista de tecnologia da informação descubra que algo foi realizado.

3.5 WORMS

O primeiro worm a chamar a atenção foi o Morris Worm, feito no Laboratório de Inteligência Artificial do MIT por Robert T. Morris Jr. Foi colocado na rede em 2 de novembro de 1988 e rapidamente infectou muitos computadores.

Os worms têm suas ações em forma de malware, bem similares às vistas anteriormente. Porém, o que chama atenção não é sua ação, e sim sua maneira de propagação.

Um worm cria cópia de si mesmo, ou seja, se retro propaga, então, enquanto seu antivírus encontra uma versão, várias outras podem estar coexistindo pela rede ou dispositivos conectados.

3.6 BOTNET

Bot é um programa que dispõe de mecanismos de comunicação com o invasor, permitindo que ele seja controlado remotamente. Possui um processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando as vulnerabilidades existentes em programas instalados em computadores.

A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

FIGURA 8 – BOOTNET

FONTE: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSUt1cUrjs0cAQk0hTN-ZGLfE179kowljdz4jbu0mDrfgy0P0Pb>. Acesso em: 31 jul. 2019.

Um computador infectado por um bot costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono.

Também é chamado de *spam zombie* quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio de spam. Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

3.7 PHISHING

O phishing pode ocorrer de diversas formas. Algumas são bastante simples, como conversas falsas em mensageiros instantâneos ou e-mails que pedem para clicar em links suspeitos. Fora isso, existem páginas inteiras construídas para imitar sites de bancos e outras instituições. Todas essas maneiras, no entanto, convergem para o mesmo ponto: roubar informações confidenciais de pessoas ou empresas.

FIGURA 9 – PHISHING

FONTE: <https://tecnologia-informatica.com/wp-content/uploads/2019/02/phishing-tipos-de-phishing-8.jpeg>. Acesso em: 10 dez. 2018.

Se você já ouviu seus amigos reclamarem que receberam e-mails de um colega pedindo para clicar em determinado link, fique atento. O mesmo pode acontecer com você. Outros casos comuns são aquelas mensagens "estranhas" que alguns usuários recebem de amigos enquanto conversam no Windows Live Messenger (antigo MSN). O funcionamento é quase igual ao dos e-mails falsos, e você precisa tentar identificar a linguagem que o seu amigo normalmente usa. Fora isso, o mesmo tipo de fraude pode acontecer também através de SMS.

Agora que você está entrando no mundo da cibersegurança verá que os nomes vistos são apenas os principais malwares e que existem diversas nomenclaturas importantes para conhecer. O site Tecmundo preparou um glossário com os principais termos da área de segurança da informação, vale a pena conferir, *Glossário do Mal: os diferentes tipos de malware que podem atingir você*, disponível em: <https://www.tecmundo.com.br/seguranca/8284-glossario-do-mal-conheca-os-diferentes-tipos-de-ataque-ao-computador.htm>.

Até o momento você aprendeu sobre os principais meios de ataques à segurança por intermédio de softwares. No segmento da segurança da informação se discutem os papéis e muito se questionam sobre quem são os hackers que desenvolvem esses softwares maliciosos e realizam ataques. Na próxima unidade você irá compreender como funciona a segurança da informação pela perspectiva de redes de computadores.

RESUMO DO TÓPICO 2

Neste tópico, você aprendeu que:

- A segurança é um atributo do sistema que reflete sua capacidade de se proteger de ataques externos, sejam acidentais ou deliberados

- Os Malwares (*Malicious* softwares) assim como diz sua tradução, são softwares maliciosos, que, independente da maneira com que chegaram ao seu dispositivo, com certeza não tem boa intenção.

- O nome vírus se dá principalmente pelo fato de se propagar rapidamente, assim como os vírus biológicos.

- O spyware é um tipo de malware denominado espião e ao contrário dos vírus não realizam nenhuma ação de danificação, e por serem programas espiões, são dificilmente detectados.

- Os *trojan horses*, ou apenas trojans, são programas de computadores denominados cavalos de Tróia, que seguem a ideia da história real. São programas de computador que realizam a função para a qual foram designados e mais alguma função maliciosa.

- Os worms têm suas ações em forma de malware, bem similares às vistas anteriormente. Porém, o que chama atenção não é sua ação, e sim sua maneira de propagação.

- Um worm cria cópia de si mesmo, ou seja, se retro propaga, então, enquanto seu antivírus encontra uma versão, várias outras podem estar coexistindo pela rede ou dispositivos conectados.

- Um computador infectado por um bot costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono.

- O phishing pode ocorrer de diversas formas. Algumas são bastante simples, como conversas falsas em mensageiros instantâneos ou e-mails que pedem para clicar em links suspeitos.

AUTOATIVIDADE

1 Analise as seguintes afirmativas referentes aos cuidados a serem tomados contra códigos maliciosos.

I- O antivírus deve ser mantido sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.
II- O antivírus deve ser configurado para verificar automaticamente os discos rígidos e as unidades removíveis (como pen drives, CDs, DVDs e discos externos).
III- O antivírus deve ser configurado para verificar toda e qualquer extensão de arquivo.

Estão CORRETAS as afirmativas:
a) ( ) I e II, apenas.
b) ( ) I e III, apenas.
c) ( ) II e III, apenas.
d) ( ) I, II e III.

2 (FCC - TRT, 2018) Considere o texto a seguir:

"Um grupo de especialistas em segurança encontrou um novo tipo de malware, que está se espalhando massivamente por meio do Facebook Messenger. Trata-se do Digmine, um malware que usa sistemas infectados para extrair a criptomoeda Monero. Esse malware é enviado às vítimas como um link para um arquivo de vídeo, quando na verdade é um script executável que afeta as versões desktop e web do Facebook Messenger, usando o navegador Google Chrome para minerar a moeda Monero no computador" (Adaptado de: https://guiadobitcoin.com.br/).

Esse tipo de malware, que parece ser uma coisa (vídeo), mas na realidade é outra (script de mineração), é categorizado como:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes?migalha=true&disciplina=46&prova=57055&modo=1>. Acesso em: 2 ago. 2019.

a) ( ) trojan.
b) ( ) backdoor.
c) ( ) adware.
d) ( ) rootkit.

3 Quando abordamos segurança da informação a nível de software é comum tratar do tema trojan. Sobre o trojan, assinale a alternativa CORRETA.

a) ( ) Os Trojans são danosos, ou seja, causam algum dano ao sistema. Estes danos geralmente são a remoção ou alteração de arquivos importantes do sistema, mas existem trojans mais zombeteiros que trocam ícones, transformam pastas em atalhos, entre outras brincadeiras de mau tom.
b) ( ) Trojans é um software que o próprio usuário instala em sua máquina com o objetivo de monitorar a atividade de outros usuários. Tem se tornado uma prática comum em empresas com a finalidade de monitorar os funcionários
c) ( ) Trojans não são exatamente um programa e se não fosse uma técnica maliciosa poderíamos dizer se tratar de um conjunto de boas práticas, mas são um conjunto de práticas maliciosas que garantem que a presença de um invasor não seja notada em um dispositivo.
d) ( ) Trojans são programas de computadores denominados cavalos de Tróia, que seguem a ideia da história real. São programas de computador que realizam a função para a qual foram designados e mais alguma função maliciosa.

4 Em um ambiente operacional existem diversos softwares. Dentre esses softwares, existe o vírus. Sobre o vírus selecione a alternativa CORRETA.

a) ( ) Os vírus são danosos, ou seja, causam algum dano ao sistema. Estes danos geralmente são a remoção ou alteração de arquivos importantes do sistema, mas existem vírus mais zombeteiros que trocam ícones, transformam pastas em atalhos, entre outras brincadeiras de mau tom.
b) ( ) Vírus é um software que o próprio usuário instala em sua máquina com o objetivo de monitorar a atividade de outros usuários. Tem se tornado uma prática comum em empresas com a finalidade de monitorar os funcionários.
c) ( ) Vírus não são exatamente um programa e se não fosse uma técnica maliciosa poderíamos dizer se tratar de um conjunto de boas práticas, mas são um conjunto de práticas maliciosas que garantem que a presença de um invasor não seja notada em um dispositivo.
d) ( ) Vírus são programas de computadores denominados cavalos de Tróia, que seguem a ideia da história real. São programas de computador que realizam a função para a qual foram designados e mais alguma função maliciosa.

SEGURANÇA EM REDES DE COMPUTADORES

1 INTRODUÇÃO

Até o momento você estudou alguns mecanismos de segurança que são garantidos a nível de sistema operacional e de software. Também pôde compreender quais são os principais softwares maliciosos e as maneiras de prevenir seus ataques.

FIGURA 10 – ATAQUES EM REDES DE COMPUTADORES

FONTE: <https://www.bizjournals.com/denver/blog/boosters_bits/2015/10/level-3-cisco-take-down-major-cybercrime-network.html>. Acesso em: 5 dez. 2018.

A partir de agora, iremos avaliar a segurança da informação pela perspectiva das redes de computadores, conhecendo as principais vulnerabilidades e como garantir a segurança a este nível.

2 SEGURANÇA EM REDE DE COMPUTADORES

O número de usuários conectados no mundo todo cresceu 1.114% desde 2010, na América do Norte e na Europa há uma estimativa de que 90% de sua população acesse a internet. O tamanho da internet também é outro que atingiu níveis muito altos. Até abril de 2019, o número de sites ativos era de aproximadamente 1.45 bilhão. Se compararmos isso com os 215 milhões de 2009, podemos dizer que a internet está quase sete vezes maior do que há dez anos.

FONTE: <https://olhardigital.com.br/noticia/dados-mostram-o-crescimento-impressionante-da-internet-em-10-anos/85914>. Acesso em: 10 dez. 2019.

Tanenbaum e Wetherall (2011, p. 18), define rede de computadores como um "conjunto de computadores autônomos interconectados por uma única tecnologia. Dois computadores estão interconectados quando podem trocar informações. Existem redes em muitos tamanhos, modelos e formas, como veremos mais adiante".

Tomando conhecimento da proporção da internet como uma rede mundial de computadores, que permite a troca de informações entre diversos dispositivos, se torna necessária a preocupação com a segurança. A internet é um lugar onde qualquer um pode estar sujeito a invasões de criminosos virtuais, espionagem de governos e de concorrentes de negócio, tudo depende de como aplicar as regras de segurança.

FIGURA 11 – IOT - CIDADES INTELIGENTES

FONTE: <https://www.wamc.org/sites/wamc/files/styles/medium/public/201801/smartcity.jpg>. Acesso em: 5 dez. 2018.

Indo um pouco além nessa reflexão sobre o papel da internet no cotidiano das pessoas, estamos em meio a uma revolução tecnológica que acontece principalmente pela Indústria 4.0, *Big Data*, Inteligência Artificial, Internet das Coisas e uma gama de novas tecnologias emergentes.

FIGURA 12 – SMART HOME

FONTE: <https://www.swann.com/blog/wp-content/uploads/2018/12/Smart-Home-Technology.jpg>. Acesso em: 5 dez. 2018.

O que todas elas têm em comum? Todas elas, de alguma maneira, utilizam conexões por intermédio de uma rede de computadores.

Estamos falando de colocar na porta uma campainha inteligente, que pode atender via smartphone, ter lâmpadas conectadas ao *Amazon Echo*, comprar uma máquina de lavar roupa que decide qual o melhor ciclo a utilizar ou até uma geladeira que controla o estoque e faz o pedido on-line quando termina, são opções desenhadas para facilitar a vida dos utilizadores. E todos esses recursos conectados.

No tópico anterior, quando falamos sobre malwares e invasões a um computador, você deve ter imaginado o vazamento de dados e informações. Quando elevamos esse pensamento para um mundo de coisas conectadas, uma invasão pode significar o controle total de dispositivos pelo invasor.

Por isso, nosso objetivo neste tópico é tratar de assuntos relativos à segurança referente ao uso de computadores pessoais e em redes corporativas, mas, também, trazer uma reflexão de como a segurança da informação é importante para o futuro da tecnologia.

Deixando as teorias da conspiração de lado, você já parou para imaginar como os robôs funcionam? É claro que muitos deles têm autonomia e não estão conectados a nenhuma rede. Todavia, uma vez estando conectados, seja para obter instruções à distância ou acessar um servidor na nuvem, consegue imaginar o que pode acontecer se esta rede for invadida?

Sendo assim, cada vez mais aumenta a preocupação com a segurança da informação, com isso chegamos à conclusão de que novas tecnologias precisam de proteção.

Evolução tecnológica pressiona mecanismos de segurança das empresas

Novas tecnologias pedem novas abordagens de proteção. Essa premissa desafia empresas ao embarcarem em ondas tecnológicas. Um estudo recente da CompTIA com 500 profissionais revelou que as organizações tentam adaptar suas políticas para acomodarem o avanço da nuvem, mobilidade e aplicativos.

A pesquisa identificou que 90% dos entrevistados avaliam que a segurança é mais importante hoje, para suas empresas, do que era há dois anos. Contudo, quase metade (47%) dos encarregados em manter ativos digitais seguros dizem que há uma crença de que os mecanismos de proteção existentes são "bons o suficiente", o que pode acarretar uma falsa sensação de segurança.

Os desafios tocam temas diversos, desde priorização de investimentos até falta de recursos humanos para lidar com contextos tecnológicos emergentes.

Pelo estudo, quatro em cada 10 entrevistados citam a falta de métricas de segurança; enquanto uma percentagem ligeiramente menor (37%) aponta para uma falta de orçamento dedicado a segurança.

A pesquisa sugere maior desafio ao encontrar trabalhadores de segurança qualificados, no momento em que a busca de competências de segurança está aumentando. A CompTIA cita aumento na busca por "Analistas de Segurança da Informação" e especialistas em cibersegurança.

Entre as empresas com lacunas de competências, 53% querem estar mais informadas sobre as ameaças atuais. Cerca de 40% sentem que precisam melhorar a sua percepção do ambiente regulatório.

Dois terços das empresas estão envolvidas na capacitação de seus funcionários com relação à segurança, tornando-se a opção principal para construir as habilidades de segurança adequadas.

FONTE: <https://computerworld.com.br/2016/06/22/evolucao-tecnologica-pressiona-mecanismos-de-seguranca-das-empresas/>. Acesso em: 10 dez. 2018.

3 SEGURANÇA EM REDES SEM FIO

As redes de computadores sem fio têm mudado o relacionamento entre computadores e máquinas, bem como a maneira de conectar as máquinas em si. Apesar de parecer uma tecnologia nova Tanenbaum e Wetherall (2011, p. 33) afirmam que:

> A comunicação digital sem fios não é uma ideia nova. Em 1901, o físico italiano Guglielmo Marconi demonstrou como funcionava um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código Morse (afinal de contas, os pontos e traços são binários). Os modernos sistemas digitais sem fios têm um desempenho melhor, mas a ideia básica é a mesma.

Poderíamos passar aqui pelos tipos de rede, as maneiras de se conectar, as estratégias. No entanto, nosso objetivo principal é o estudo de questões de segurança a nível de rede, de todo modo, deixaremos uma sugestão de leitura para que você possa aprofundar seus conhecimentos.

Leia o livro sobre conhecimentos em redes de computadores: COMER, Douglas E. **Redes de computadores e internet**. 6. ed. Porto Alegre: Bookman Editora, 2016.

Complementarmente estamos vivendo na década da mobilidade, sendo puxada principalmente por redes Wi-Fi, 4G (em algumas cidades já existe 5G) e Bluetooth. Isto tem acontecido por diversos fatores, um deles citados anteriormente, IoT que faz aumentar o número de conexões Bluetooth entre dispositivos.

Se você foi recentemente a algum estabelecimento comercial, dificilmente não se conectou ao Wi-Fi de lá utilizando sua rede social ou até mesmo em uma rede aberta (sem senha). Nos últimos anos, este tipo de rede tem se tornado comum, principalmente para prover comodidade aos clientes e visitantes dos mais diversos tipos de comércio.

FIGURA 13 – WI-FI ZONE

FONTE: <https://s3.ap-southeast-1.amazonaws.com/images.deccanchronicle.com/dc-Cover-rfmrujmn5pogpvtgavrnn8p9h4-20180508175455.Medi.jpeg>. Acesso em: 5 dez. 2018.

Afinal, será que é seguro se conectar às redes desses estabelecimentos? O ponto é, não há como saber o nível de segurança, e, principalmente, saber quem está conectado a ela.

> Segundo Thiago Hyppolito, engenheiro de produtos da McAfee no Brasil, cibercriminosos costumam aproveitar falhas de segurança (às vezes dos próprios roteadores, aparelhos que distribuem a internet) para bisbilhotar as atividades on-line dos usuários. "A interceptação de dados não requer muito conhecimento de computação. Qualquer curioso acha um tutorial na rede ensinando isso", disse Hyppolito. "O atacante fica monitorando a rede à espera de transações bancárias ou de login em redes sociais" (TAGIAROLI, 2015, s.p.).

Neste sentido, quando acessar redes públicas, o recomendável é acessar somente o básico, evitando acesso a dados bancários ou informações sigilosas.

Você conhece o que é um roteador? Imagino que pelo menos uma vez deve ter configurado um e se ainda não o fez, o fará. O processo de configuração de um roteador é relativamente simples e a grande maioria dos roteadores do mercado vêm prontos para serem ligados e já funcionarem.

Hoje em dia os roteadores do mercado acumulam diversas outras funções, mas a principal é compartilhar conexão entre vários dispositivos. Sendo, então, essencial para qualquer rede de computadores.

Durante o Tópico 1, você conheceu o termo criptografia e seu importante papel para a segurança da informação, cada protocolo de rede atua sob uma maneira de criptografar. Ou seja, cada um armazena a senha de acesso ao roteador com uma estratégia de criptografia. Vamos conhecer um pouco mais sobre eles.

4 WEP

O WEP – *Wired Equivalent Privacy*, tem como tradução aproximada "privacidade equivalente a uma rede cabeada", no decorrer do estudo você verá que não é bem assim. Segundo Vilela *et al*. (2013, p. 146):

> O primeiro protocolo de segurança lançado pela IEEE 802.11 foi o WEP (*Wired Equivalence Privacy*) em 1999. Este se mostrou muito vulnerável a ataques de negação de serviço e ataques de força bruta devido à chave de criptografia ser reduzida, reutilizada e estática. Em 2003 houve a primeira atualização na ementa de segurança do IEEE 802.11, sendo assim, foi implantado o protocolo WPA (Wi-Fi Protected Access) apenas como solução temporária, enquanto o desenvolvimento da nova ementa era finalizado. Em 2004 foi lançado o IEEE 802.11i. Em 2009, foi implementado padrão de segurança denominado IEEE 802.11w, este por sua vez adiciona proteção em alguns quadros de gerenciamento, mas ainda não protegia os quadros de controle.

O WEP foi o primeiro protocolo de autenticação, apesar de alguns roteadores, principalmente os mais antigos, virem com esta opção, hoje não é mais utilizado, pois os ataques são bem conhecidos e é muito fácil de ser quebrado.

Segundo Rufino (2005 *apud* RIOS, 2012, p. 72):

> WEP é um protocolo que utiliza algoritmos simétricos; portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o concentrador, para cifrar e decifrar as mensagens trafegadas". Os critérios que foram levados em consideração para o desenho do protocolo foram ser suficientemente forte, auto sincronismo, requerer poucos recursos computacionais, exportável e de uso opcional.

Ainda sobre as falhas deste protocolo, o FBI – *Federal Bureau of Investigation* realizou uma demonstração pública no ano de 2005. Durante a demonstração realizaram quebra de chaves WEP (descoberta de senhas) com ferramentas gratuitas, visando avisar sobre as falhas no protocolo, que, na época, era o mais utilizado no mundo.

5 WPA

O WPA (*Wi-Fi Protected Accesc*), algo como Wi-Fi de acesso protegido, assumiu o lugar quando a WEP começou a sair de circulação. É muito comum que a literatura traga o WPA como a "versão melhorada do protocolo Wep".

A adoção inicial foi no ano 2003, quando a novidade era a criptografia em 256 bits, sendo uma promessa para aumentar a segurança. O protocolo também implementa métodos de análise de pacotes, o que permite analisar e tentar descobrir invasões.

Grande parte dos especialistas culpa às falhas existentes no WPA na herança do WEP, pois alguns recursos do protocolo não ficaram obsoletos e foram reaproveitados.

Protocolos de segurança de rede sem fio: WEP, WPA e WPA2

O WPA foi uma melhoria significativa sobre o WEP, mas como os principais componentes foram feitos para que eles pudessem ser implementados através de atualizações de firmware em dispositivos habilitados para WEP, ele ainda se baseava em elementos vulneráveis.

Assim como WEP, depois de ter sido submetido a uma prova de conceito e aplicado a demonstrações públicas acabou, por sua vez, sendo muito vulnerável a invasões. Os ataques que representavam a maior ameaça para o protocolo, não eram feitos diretamente, mas sim através do sistema Wi-Fi Protected Setup (WPS) - sistema auxiliar desenvolvido para simplificar a conexão dos dispositivos aos pontos de acesso modernos.

FONTE: <https://www.netspotapp.com/pt/wifi-encryption-and-security.html>. Acesso em: 12 dez. 2018.

5.1 WPA2

O sistema-padrão atual e o mais seguro, implementado pela Wi-Fi Alliance em 2006. A diferença aqui é a maneira como o sistema lida com senhas e algoritmos, excluindo completamente a possibilidade de um ataque de força bruta. Sendo assim, este é o tipo mais seguro da atualidade. Segundo especialistas, o risco de intrusões para usuários domésticos com WPA2 é praticamente zero.

Isso se deve a duas outras siglas incompreensíveis. O AES (Advanced Encryption Standard), um novo padrão para a segurança das informações, e o CCMP (Counter Cipher Mode), um mecanismo de encriptação que protege os dados que passam pela rede. O WPA2 é tão complexo que muitos dispositivos, mesmo recentes, não são compatíveis com ele.

Uma das poucas vulnerabilidades conhecidas atinge diretamente usuários corporativos e exige que o atacante possua acesso normal à rede sem fio. Uma vez conectado, o hacker poderia assumir o controle de outros dispositivos ligados à rede, incluindo dados contidos neles ou transferidos a partir das máquinas. Mais uma vez, isso se deve a programações de compatibilidade para ligação de roteadores antigos e modernos.

FONTE: DEMARTINI, F. WEP, WPA, WPA2: o que as siglas significam para o seu wi-fi? **TecMundo**, São Paulo, jul. 2013. Disponível em: https://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm. Acesso em: 31 jul. 2019.

6 AES

AES (*Advanced Encryption Standard*) é um padrão autorizado de encriptação forte para redes Wi-Fi.

> O AES é uma primitiva criptográfica destinada a compor sistemas de cifragem e decifragem simétrica (i.e. mesma, chave para cifrar e decifrar). É uma cifra de bloco, ou seja, opera em blocos de tamanho fixo (128 bits, ou 16 bytes). Como toda cifra de bloco, pode ser transformada numa cifra de fluxo (de modo a operar em dados de tamanho arbitrário) através de um modo de operação, mas isso não vem ao caso aqui. Pode trabalhar com chaves de 128, 192 ou 256 bits.
>
> Em outras palavras, é um algoritmo cuja função direta (cifragem) recebe como entradas um bloco de 128 bits (a mensagem) e uma chave do tamanho escolhido, e devolve uma saída também de 128 bits (a cifra). A função inversa (decifragem) recebe como entrada um bloco de 128 bits (a cifra) e devolve como saída um bloco de 128 bits. Se a chave for a chave correta, essa saída será idêntica à mensagem original.

> O objetivo de uma cifra bem-sucedida é que seja impraticável se descobrir a mensagem original caso somente se possua a mensagem cifrada, mas não a chave de criptografia. Para isso, busca-se minimizar qualquer correlação visível entre a entrada e a saída, de modo que a mesma (e/ou a chave) possa ser deduzida simplesmente observando-se um número muito grande de cifras (ou de pares mensagem/cifra). Para isso, usa-se uma série de "rodadas" (ou rounds) em que os bytes sofrem transformações não lineares, porém reversíveis (i.e., para decifrar, simplesmente se executa o inverso das mesmas operações, em ordem inversa) (COSTA; LANGER JÚNIOR, 2015, p. 27).

Além da melhor configuração, recomenda-se, ainda, ficar atento para algumas condições que podem parecer seguras, mas que na verdade não são. Por exemplo:

- Esconder o nome da rede: isso, apesar de impedir que pessoas não autorizadas localizem e tentem se conectar a sua rede, faz também com que seu computador esteja constantemente buscando a sua conexão e divulgando o nome dela por aí. E esse sinal, nas mãos de uma pessoa que saiba identificá-los, permite que elas acessem sua rede normalmente;
- Filtragem de MAC: todo dispositivo de acesso Wi-Fi possui um endereço próprio, chamado MAC, que o identifica na rede. Qualquer roteador possui sistemas de proteção que permitem apenas o acesso de máquinas autorizadas. Ainda assim, porém, é possível para qualquer um verificar quais são os endereços dos dispositivos conectados e maquiar a própria identidade para se parecer com um deles;
- IP fixo: roteadores designam automaticamente os IPs para cada máquina conectada. Para muita gente, porém, desabilitar essa função seria uma forma de controle, já que depende de uma inserção manual de dados a cada nova conexão. O único problema disso é que uma rápida busca no Google já é capaz de ensinar como modificar ou dar um número à própria máquina (DEMARTINI, 2013, s.p.).

Agora que estamos próximos de encerrar mais uma unidade, é importante você saber que, muitas vezes, o profissional de segurança da informação tem que andar pelo "lado negro da força" para aprender como se defender. Isto significa que você terá que desenvolver algumas habilidades de atacante para garantir a segurança da sua rede.

Por isso, para atuar como profissional de segurança é preciso, além de grande responsabilidade, agir com ÉTICA a todo momento.

Sendo assim, você aprenderá sobre algumas ferramentas do mercado e espero que as utilize com sabedoria, profissionalismo e ética.

LEITURA COMPLEMENTAR

PROFISSÃO: ESPECIALISTA EM SEGURANÇA DA INFORMAÇÃO

TecMundo

Proteger a integridade de dados sigilosos, sejam eles de pessoa física ou jurídica, contra aquisições inapropriadas e fraudes é dever dos profissionais especializados em segurança da informação. Mas no que consiste esta profissão? Quais são as áreas de atuação? Que características um profissional deve ter para se especializar em segurança informacional? Descubra a importância dos "xerifes" do mundo virtual.

O que ele faz?

Segundo a NBR ISO/IEC 17799 (ABNT, 2005, p. IX), a segurança da informação consiste na "proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

Para que isso seja alcançado existem formas de controlar o trâmite desse conteúdo. De acordo com a norma citada anteriormente, estão inclusos nesses conjuntos de ferramentas gerenciais a definição de políticas de acesso, a estipulação de processos e procedimentos que resguardem a integridade dos dados armazenados, consolidação de estruturas organizacionais bem definidas e implementação de funções de software e hardware.

Obviamente, estes recursos devem ser monitorados, analisados criticamente e aperfeiçoados com o objetivo de minimizar ao máximo qualquer brecha na segurança e gestão informacional, assegurando que os objetivos de negócio sejam alcançados.

Como se pode perceber, não basta instalar um antivírus e colocar uma senha no log on do sistema operacional para que as preciosas informações, para você ou sua empresa, fiquem a salvo dos crimes digitais que assolam a sociedade contemporânea.

Em outras palavras, o profissional especializado em segurança da informação deve prevenir que dados sigilosos sejam roubados ou vazem para os concorrentes. Os "xerifes" da Era da Informação têm as missões de, segundo Marcos Vinícius da Silva Junior (arquiteto da informação da *Kahuna Security*):

- Assegurar a disponibilidade dos recursos informacionais.
- Resguardar a integridade das informações.
- Garantir a confidencialidade do conteúdo.

Áreas de atuação e o mercado de trabalho

Uma das preocupações mais comuns entre os jovens que estão se preparando para escolher uma profissão é o mercado de trabalho. Basicamente, um profissional especializado em segurança da informação pode atuar com a elaboração de planos estratégicos que resguardem os dados e informações, a auditoria de sistemas informatizados e o monitoramento e controle de políticas de segurança.

Os postos mais comuns para estes profissionais são a educação corporativa (relacionada à segurança computacional), análise de códigos maliciosos (muito procurado por empresas de antivírus) e desenvolvimento de produtos e serviços.

Essas atividades não são as únicas, qualquer função que envolva o estudo de maneiras que garantam a integridade de informações é válida, como a perícia forense – órgãos da administração pública que visam coordenar atividades contra crimes cibernéticos. Já pensou em se tornar um policial científico como os personagens da série de TV norte-americana chamada CSI? Com conhecimentos em segurança informacional e os devidos processos seletivos, você pode ser o Gil Grissom brasileiro!

Isso soou como exagero? Mas a verdade é que a ABIN (Agência Brasileira de Inteligência) possui células de defesa nacional que são responsáveis pela segurança das informações e dos conhecimentos sigilosos do Governo. Como é de se esperar, o processo para alcançar cargos nestes departamentos são extremamente rigorosos, ou você pensa que é fácil se tornar um agente secreto ao melhor estilo do James Bond?

Outro aspecto muito especulado é a faixa salarial para um profissional com formação em segurança da informação. No início de carreira os salários ficam em torno de R$2.500, mas não existem limites – devido ao crescimento da área e escassez de mão de obra. Veja na tabela a seguir alguns dos valores pagos aos cargos mais avançados, segundo a *Desix Software Solution*:

Cargo	Salário em R$		
	Júnior	Pleno	Sênior
Analista de segurança de informações	R$ 4.406,00	R$ 4.588,00	R$ 6.488,00

FONTE: Desix Software Solution

A importância deste profissional

Nunca ouviu falar nesta profissão? Realmente, para boa parte da população esta função é desconhecida. Isso não diminui ou menospreza a importância que este profissional tem para a sociedade. A tarefa de garantir a integridade de dados e sistemas, por consequência, das operações em níveis táticos e estratégicos tem sido vista com bons olhos pelas organizações – principalmente as privadas.

Quando a informática começou a se popularizar e ficar mais acessível para as empresas, todos os recursos informacionais eram armazenados em um único departamento, o clássico CPD (Centro de Processamento de Dados). Essa centralização facilitava muito o controle de acesso e movimentos das informações.

Entretanto, esse contexto já está muito mais que ultrapassado. Atualmente, smartphones, computadores portáteis, serviços de e-mail e pen drives são mecanismos que aumentam a vulnerabilidade do conhecimento corporativo. Dados financeiros, cadastro de clientes e outras informações de cunho estratégico rodam livremente fora das dependências das empresas.

Ao contrário do que muitas pessoas imaginam, a espionagem industrial não é um mero tema cinematográfico (como retrata o filme *O Informante*), ela acontece entre as corporações de grande porte.

Características essenciais

Com certeza alguns aficionados por tecnologia devem ter sentido vontade de se tornar um "xerifão" das informações. Porém, é válido deixar todos avisados que essa não é uma missão das mais fáceis. Um bom profissional deve ter amplos conhecimentos nos mais variados assuntos relacionados com tecnologia e aspectos legais da área.

Para isso, muito estudo, dedicação e manter-se antenado com o mundo da informática é essencial para que você seja um especialista em segurança da informação com gabarito. Para quem se interessou pela profissão, existem informações mais detalhadas no site da ASAP (*Alliance of Security Analysis Professionals*), associação de profissionais especializados em análises de segurança.

FONTE: <https://www.tecmundo.com.br/seguranca/5366-profissao-especialista-em-seguranca-da-informacao.htm>. Acesso em: 10 dez. 2018.

RESUMO DO TÓPICO 3

Neste tópico, você aprendeu que:

- O número de usuários conectados no mundo todo cresceu 1.114% desde 2010, na América do Norte e na Europa há uma estimativa de que 90% de sua população acesse a internet.
- Rede de computadores é um conjunto de computadores autônomos interconectados por uma única tecnologia.
- Cada vez mais aumenta a preocupação com a segurança da informação, com isso chegamos à conclusão de que novas tecnologias precisam de proteção.
- As redes de computadores sem fio têm mudado o relacionamento entre computadores e máquinas, bem como a maneira de conectar as máquinas em si.
- A rede Wi-Fi tem se tornado comum, principalmente para prover comodidade aos clientes e visitantes dos mais diversos tipos de comércio.
- O WEP — *Wired Equivalent Privacy* — foi o primeiro protocolo de autenticação, apesar de alguns roteadores, principalmente os mais antigos, virem com esta opção, hoje não é mais utilizado, pois os ataques são bem conhecidos e é muito fácil de ser quebrado.
- O WPA (*Wi-Fi Protected Accesc*), algo como Wi-Fi de acesso protegido, assumiu o lugar quando a WEP começou a sair de circulação. É muito comum que a literatura traga o WPA como a "versão melhorada do protocolo Wep".
- O WPA2 é a maneira como o sistema lida com senhas e algoritmos, excluindo completamente a possibilidade de um ataque de força bruta. Sendo assim, este é o tipo mais seguro da atualidade.
- O AES (*Advanced Encryption Standard*) é um padrão autorizado de encriptação forte para redes Wi-Fi.

Ficou alguma dúvida? Construímos uma trilha de aprendizagem pensando em facilitar sua compreensão. Acesse o QR Code, que levará ao AVA, e veja as novidades que preparamos para seu estudo.

AUTOATIVIDADE

1 Os protocolos WEP, WPA e WPA2 podem ser utilizados na segurança de redes sem fio. Analise as proposições a seguir e marque a assertiva CORRETA.

a) ( ) A sigla WEP significa *Wireless Equivalent Privacy*.
b) ( ) O protocolo WEP é mais seguro que o protocolo WPA.
c) ( ) *WPA-Personal* (ou WPA-PSK) foi projetado para ambientes pequenos e não requer um servidor para autenticação (por exemplo, RADIUS).
d) ( ) O protocolo WPA não pode ser utilizado com o protocolo 802.1X.

2 Vivemos em uma era de avanços tecnológicos, se fala de *Big Data*, Internet das Coisas, Indústria 4.0, entre outros. Sobre segurança da informação e novas tecnologias selecione a alternativa CORRETA.

a) ( ) Como tais tecnologias não dependem de redes de computadores, não há preocupação com segurança.
b) ( ) A preocupação com segurança deve ser ampliada, para um mundo de coisas conectadas, uma invasão pode significar o controle total de dispositivos pelo invasor.
c) ( ) Deve-se desconectar os dispositivos da rede para poder garantir segurança total.
d) ( ) Deve-se sempre utilizar protocolo WPA.

3 A disponibilização de internet em locais públicos tem sido cada vez mais comum no cotidiano dos brasileiros. Todavia, a maioria dos utilizadores parecem esquecer das partes negativas que esta facilidade traz. Sobre a utilização deste tipo de rede, selecione a alternativa CORRETA.

a) ( ) A segurança é sempre garantida pelo proprietário.
b) ( ) Sempre é melhor se conectar quando a rede for aberta (não pedir autenticação).
c) ( ) Nesse tipo de rede, o atacante pode estar monitorando a rede à espera de transações bancárias ou de log in em redes sociais.
d) ( ) Deve-se sempre confiar em redes que utilizam as informações de log in e senha.

4 Para garantir melhor segurança em redes sem fio são utilizadas chaves de criptografia. A escolha de uma opção errada, e você terá uma rede mais lenta e menos segura. Apesar dos nomes estranhos e das possibilidades de problemas, essa configuração é importante e deve ser escolhida com calma, e claro, com algum conhecimento das tecnologias envolvidas. Selecione a alternativa CORRETA que contenha os principais tipos de criptografia.

a) ( ) WEP, WPA, WPA2.
b) ( ) SQL, DBA, DB2.
c) ( ) Rj45, WPA, WPA2.
d) ( ) WEB, DB2, WWW.

UNIDADE 3

NORMAS E GESTÃO DE SEGURANÇA DA INFORMAÇÃO

OBJETIVOS DE APRENDIZAGEM

A partir do estudo desta unidade, você deverá ser capaz de:

- conhecer as principais leis, normas e padrões de segurança da informação aplicáveis no mercado atual;
- compreender as principais características de uma política de segurança da informação e do plano de continuidade de negócio;
- entender a aplicação da segurança da informação na rotina diária de uma organização, incluindo, por exemplo, o controle de acesso e auditorias;
- conhecer os principais aspectos humanos envolvidos, assim como suas necessidades e recomendações ao lidar com segurança da informação

PLANO DE ESTUDOS

Esta unidade está dividida em quatro tópicos. No decorrer da unidade, você encontrará autoatividades com o objetivo de reforçar o conteúdo apresentado.

TÓPICO 1 – LEGISLAÇÃO, NORMAS E PADRÕES DE SEGURANÇA DA INFORMAÇÃO

TÓPICO 2 – POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PLANO DE CONTINUIDADE DE NEGÓCIO

TÓPICO 3 – ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO E CONTROLE DE ACESSO

TÓPICO 4 – AUDITORIA, SEGURANÇA FÍSICA E DO AMBIENTE

Preparado para ampliar seus conhecimentos? Respire e vamos em frente! Procure um ambiente que facilite a concentração, assim absorverá melhor as informações.

LEGISLAÇÃO, NORMAS E PADRÕES DE SEGURANÇA DA INFORMAÇÃO

1 INTRODUÇÃO

Assim como apresentado na Unidade 1, os controles de segurança da informação estão intimamente relacionados à definição de qualidade e aos níveis organizacionais de forma que, para que haja segurança em todos os níveis da organização, será necessário a definição e utilização de políticas, normas, padrões e procedimentos de segurança da informação. Considerando que, quando se fala de todos os níveis organizacionais, entende-se, também, que isso se aplica às pessoas, processos e tecnologias relacionados àquele nível.

Ainda relembrando o que vimos até aqui, as normas, padrões, procedimentos e processos visam definir como as propriedades de segurança da informação (confidencialidade, integridade, disponibilidade, autenticidade, não repúdio, confiabilidade, entre outros) serão garantidas e realizam toda a gestão do risco, com o estudo sobre as ameaças, vulnerabilidades e medidas protetivas relacionados à segurança lógica, física e ambiental.

Enquanto na primeira unidade foi apresentado a fundamentação em segurança da informação e na segunda foi a segurança operacional em redes e os invasores, o foco desta unidade é apresentar os principais documentos a serem definidos e aplicados em uma organização, iniciando com as normas internacionais.

Em segurança da informação existem normas, padrões e procedimentos a serem seguidos e certificados, como, por exemplo, a ISO/IEC 27001. Adotar um padrão de segurança reconhecido internacionalmente significa melhorar as operações, uniformizar os processos, reduzir os riscos, averiguar métricas, entre outros benefícios.

Neste tópico será apresentada a principal família de normas internacionais e sua correspondente brasileira, alguns outros padrões utilizados, além das principais grandes leis brasileiras a respeito de segurança da informação.

2 PADRÃO ISO/IEC 27000

Depois de algumas décadas de história e aprimoramentos, em 2005, a ISO/IEC dá início a uma série direcionada à padronização de normas para o segmento de segurança da informação, lançado como padrão ISO/IEC 27000. Essa família de normas continuou evoluindo, gerando mais de uma dezena de normais, tais como:

- ISO/IEC 27000: princípios e vocabulário utilizados nas normas seguintes da família 27000.
- ISO/IEC 27001: requisitos para um Sistema de Gestão de Segurança da Informação (SGSI).
- ISO/IEC 27002: boas práticas para controles de segurança da informação.

A ISO, assim como outras entidades internacionais, certifica organizações. Esta certificação existe para identificar empresas que estão em conformidade com suas normas, ou seja, estão de acordo e seguem todas as recomendações de determinada norma. Para isso, existe um processo no qual a empresa é avaliada para analisar se atende aos requisitos das normas correspondentes ao seu nicho de atuação garantindo, assim, os padrões internacionais. De forma similar, existem certificações pessoais em segurança da informação. Ao fim desta unidade é apresentado um artigo sobre o tema. Inclusive, é possível seguir carreira como auditor da ISO.

Enquanto a ISO/IEC são entidades internacionais, a ABNT (Associação Brasileiras de Normas Técnicas) é o órgão responsável pela elaboração das Normas Brasileiras (ABNT NBR) e as distribui através da sua comercialização.

Para ter acesso e poder ler e consultar as normas, a pessoa ou instituição deve comprá-las através do site da ABNT (http://www.abnt.org.br).

A seguir, serão apresentadas as três primeiras normas da família ISO 2700. É importante atentar-se ao fato de que a forma mais justa e específica de nomear cada norma é possuir todas as entidades principais que são responsáveis por ela, seguindo da sua numeração e o ano de lançamento da versão, por exemplo, ABNT NBR ISO/IEC 27000:2018. Entretanto, por questão de simplificação, neste livro utilizaremos somente ISO 27000, considerando sempre a versão mais recente referenciada aqui.

2.1 ISO 27000

Esta norma apresenta as demais normas da família 27000, apresentando a nomenclatura de cada uma delas, dá uma visão geral sobre um SGSI (Sistema de Gestão de Segurança da Informação), destacando a sua importância e como implementá-lo e, também, especifica o vocabulário e definições de termos de segurança da informação utilizados nas normas desta família (ABNT, 2018b), que já viemos fazendo ao longo deste livro.

Assim como apresentado na Unidade 1, esta norma também define confidencialidade, integridade e disponibilidade como os pilares de segurança da informação, sendo que o SGSI é o sistema de gestão cujo objetivo é auxiliar na garantia destas propriedades (ABNT, 2018b). A ISO 27001 é responsável pelas principais definições sobre o SGSI, que veremos a seguir.

2.2 ISO 27001

Esta norma apresenta os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI dentro do contexto da organização, também inclui os requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para a necessidade da organização (ABNT, 2013a). Em resumo, apresenta os requisitos para um SGSI.

O SGSI, em si, inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação (PALMA, 2016), ou seja, define o que é necessário para gerir todo o ciclo de vida da informação no que diz respeito a sua segurança.

Observe que um SGSI não precisa ser necessariamente um sistema automatizado. A norma define que um SGSI consiste nas políticas, procedimentos, diretrizes, recursos associados e atividades, gerenciados coletivamente por uma organização, na busca de proteger seus ativos de informação.

Com o SGSI em conformidade com a ISO 27001, alguns benefícios são garantidos. Segundo Tüv Rheinland (2020), um dos principais benefícios é a redução das possibilidades de falhas de segurança dentro do ambiente de segurança da informação, devido a todo o levantamento e planejamento a respeito. Outro benefício é a minimização de riscos, de possíveis prejuízos e de custos indiretos com a segurança da informação e, consequentemente, redução dos custos devido à menor possibilidade de falhas de segurança. Além disso, também traz a possibilidade da certificação internacional, trazendo uma vantagem competitiva devido ao reconhecimento da norma e um aumento da confiança no que diz respeito a parceiros, clientes e público.

Pandini (2020) cita os principais fundamentos para a garantia de sucesso na implementação de um SGSI. O primeiro diz respeito a algo que já discutimos neste livro, o fator humano.

Deve-se criar consciência sobre a necessidade de segurança da informação, para evitar a falha por todos aqueles envolvidos. É necessário, também, estabelecer responsáveis pela segurança da informação, que tenha como função a gestão da segurança da informação. E é necessário avaliar criteriosamente os riscos, para estabelecimento de controles apropriados e obtenção de níveis aceitáveis para organização, como através da matriz de risco, já estudada na Unidade 1.

Ainda segundo Pandini (2020), deve-se tratar a segurança da informação como elemento essencial nas redes e sistemas, não de forma secundária, assim como é preciso atuar de forma ativa na prevenção e detecção de incidentes de segurança da informação. Por fim, para garantir o sucesso na implementação de um SGSI é necessário garantir uma abordagem global da gestão de segurança da informação, ou seja, ampla, analisando todos os aspectos da organização, além de estabelecer métodos de avaliação contínua, promovendo modificações de acordo com as necessidades do negócio.

Uma organização precisa executar quatro etapas para implantar, monitorar, manter e aprimorar o seu SGSI (ABNT, 2018b). A primeira é identificar os ativos de informações e seus requisitos de segurança de informações através da análise do valor da informação, da necessidade do negócio e da legislação.

A segunda etapa é avaliar os riscos à segurança da informação, a qual inclui a análise e avaliação dos riscos, identificando aqueles que podem, ou não, ser aceitos.

Na próxima etapa, então, trata-se os riscos levantados e avaliados anteriormente, através da aplicação de controles para redução desses riscos, análise e revisão dos critérios de aceitação, formas de evitá-los e/ou formas de compartilhar esses risos com as seguradoras.

Selecionar e implementar controles relevantes para gerenciar riscos inaceitáveis, os quais serão estudados no próximo tópico e, por fim, na última etapa, monitora-se manter e melhorar a eficácia dos controles associados aos ativos de informação através de métricas e evidências de verificação e rastreabilidade para ações corretivas, preventivas e de melhoria.

Para executar essas etapas descritas anteriormente é recomendado utilizar um modelo conhecido como "*Plan-Do-Check-Act*" (PDCA), tão conhecido e utilizado em sistemas de gestão. Segundo Faria (2020, s.p.), o PDCA é definido como:

> [...] um método amplamente aplicado para o controle eficaz e confiável das atividades de uma organização, principalmente aquelas relacionadas às melhorias, possibilitando a padronização nas informações do controle de qualidade e a menor probabilidade de erros nas análises ao tornar as informações mais entendíveis.

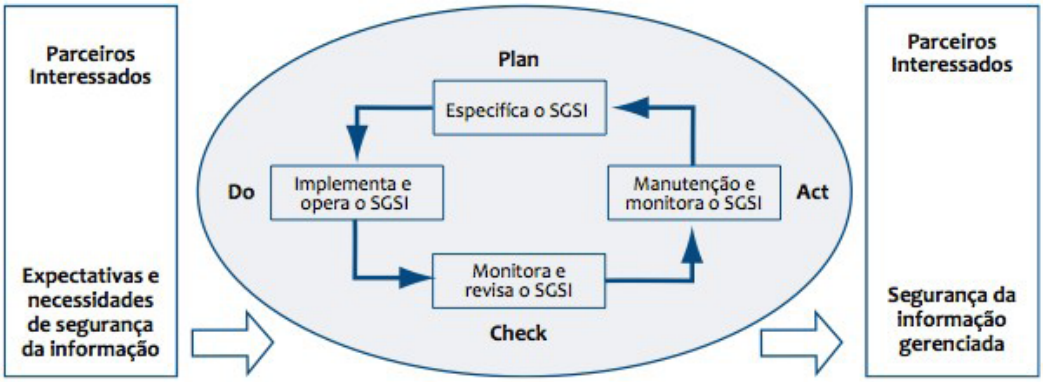
No PDCA, as partes interessadas, também chamadas de stakeholders, apresentam suas expectativas e requisitos como entrada no processo, que inicia o ciclo de Plan (planejar), Do (fazer), Check (checar) e Act (agir). Este ciclo é executado de forma cíclica até a concretização de expectativas e requisitos para então ter o objetivo conquistado como saída do processo.

Por exemplo, no caso de um treinamento a respeito das práticas de segurança para novos funcionários, na etapa **Planejar**, delineia-se as mudanças que, neste caso, seriam a preparação do cronograma de treinamento. A etapa **Fazer** corresponde à colocar em prática, ou seja, realizar o treinamento de segurança. Na próxima etapa, **Checar**, deve-se verificar se surtiu o efeito desejado, verificando se os funcionários aprenderam o conteúdo. E, na última etapa, **Agir**, em caso de o objetivo ter sido alcançado, institucionalizar a prática e, em caso negativo, identificar os fatores que impediram o objetivo de ser alcançado.

Neste caso, stakeholders, ou partes interessadas, são todos aqueles que têm interesse, afetam ou são afetados por aquele processo que está sendo gerenciado. Por exemplo: gestores, acionistas, grupos, instituições etc.

O PDCA aplicado à norma ISO 27001 na gestão do SGSI é apresentado na figura a seguir e descrito logo em seguida.

FIGURA 1 – MODELO PDCA APLICADO AO PROCESSO DO SGSI



FONTE <https://i1.wp.com/www.diegomacedo.com.br/wp-content/uploads/2012/03/Modelo-PDCA-aplicado-ao-processo-do-SGSI.png?w=602&ssl=1>. Acesso em: 5 ago. 2020.

Na sequência, encontra-se a aplicação do ciclo PDCA na ISO 27001.

QUADRO 1 – PDCA

Plan (planejar) – estabelecer o SGSI	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos da organização.
Do (fazer) – implementar e operar o SGSI	Implementar e operar a política, como a PSI que será apresentada em breve, controles, processos e procedimentos do SGSI.
Check (checar) – monitorar e analisar criticamente o SGSI	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act (agir) – manter e melhorar o SGSI	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

FONTE Adaptado de Macêdo (2012)

Um exemplo de requisito de segurança da informação para a entrada do processo é para que as violações de segurança da informação não causem sérios danos financeiros e/ou constrangimentos à organização (ABNT, 2013a). E um exemplo de expectativa é para que se caso ocorra um incidente grave, haveriam pessoas com treinamento suficiente nos procedimentos apropriados para minimizar o impacto (ABNT, 2013a).

Diversos segmentos do mercado, dentro de suas especificidades, têm a obrigatoriedade de seguir as normas, definidas pelos órgãos reguladores, que padronizam e normatizam os processos. E com a segurança da informação não seria diferente (PAZ, 2019). Mas não é somente uma questão de obrigatoriedade, as normas da família 27000 são recomendações internacionais de como tratar a segurança da informação, foram escritas por especialistas em cada um dos assuntos e vem sendo revisadas há décadas. Ou seja, seguir estas normas não é somente uma questão de conformidade, mas principalmente de minimização dos riscos na gestão do ativo mais importante do século XXI: a informação.

Para estar com o SGSI em conformidade, a norma ISO 27001 define sete grandes áreas de requisitos: Contexto da Organização, Liderança, Planejamento, Apoio, Operação, Avaliação de Desempenho e Melhoria, sendo que cada um deles apresentam vários pontos a serem considerados.

Esses requisitos são definidos de forma genérica para poderem ser aplicados em qualquer organização, independentemente de porte ou setor. E para estar em conformidade com a norma não é aceitável exclusão de quaisquer destes requisitos.

A primeira área de requisitos, **Contexto da Organização**, refere-se ao entendimento da organização e seu contexto como questões internas, por exemplo: a estrutura organizacional e recursos disponíveis, e externas, como leis e regulamentações, que são relevantes para o seu propósito e relevantes ao SGSI, assim como entender as necessidades e as expectativas das partes interessadas. Refere-se, também, à determinação do escopo do SGSI, por exemplo: para fins de certificação ou mesmo uma auditoria, definindo os limites e a aplicabilidade dele, além de estabelecer, implementar, manter e continuamente melhorá-lo.

A segunda é a **Liderança**, e diz respeito, principalmente, com o que a alta direção da organização deve fazer, como demonstrar liderança e comprometimento em relação a todo o ciclo de vida do SGSI, assegurando os recursos necessários, orientando e apoiando, entre outros pontos. Esta

liderança inicia-se pelo estabelecimento da PSI, como será abordado no Tópico 2 desta unidade, e assegurar que os papéis e responsabilidades relevantes sejam atribuídos e comunicados, como será abordado no Tópico 3.

A próxima área de requisitos é o **Apoio**, a qual define que a organização tem que determinar e prover os recursos para todo o processo do SGSI. Também precisa determinar e assegurar as competências necessárias das pessoas que realizam o trabalho, com treinamentos, por exemplo, além de trabalhar na conscientização da segurança da informação através das comunicações internas e externas a respeito.

Outra grande área é a **Operação**, ela determina que a organização precisa planejar, implementar e controlar os processos necessário para atender aos demais requisitos. Deve haver, também, avaliações de riscos de segurança da informação em intervalos planejados ou quando grandes mudanças ocorrerem. Além de possuir um plano de tratamento para os riscos encontrados.

A próxima grande área de requisitos é a **Avaliação de Desempenho**, nela avalia-se o desempenho de segurança da informação e a eficácia do SGSI através do monitoramento, medição, análise e avaliação dos processos relacionados através, por exemplo, da análise de relatórios de resposta a incidentes. Similar às avaliações de risco, é necessário que haja, também, auditoria interna periódica para prover informações quanto ao SGSI. E, novamente em intervalos definidos ou sob demanda, a alta direção deve realizar análise crítica do SGSI para assegurar a sua contínua adequação, pertinência e eficácia.

Outra área é a **Melhoria**, a qual determina que se toma a devida ação corretiva quando houver alguma não conformidade, como quando não é atendido algum requisito de segurança. Assim como a organização tem que melhorar, continuamente, a pertinência, adequação e eficácia do SGSI por meio do uso da PSI, resultados de auditorias e análise de eventos monitorados, por exemplo.

Por fim, a última grande área de requisitos faz referência quanto ao **Planejamento** do SGSI. Aqui se estabelece os objetivos de segurança da informação e o planejamento para conseguir alcançá-los. E, considerando o contexto da organização, suas necessidades e expetativas das partes interessadas, a organização deve determinar os riscos e as oportunidades, definindo e aplicando um processo de avaliação e tratamento de riscos através de controles. Estes controles e seus objetivos a serem implementados são os descritos na ISO 27002, que estudaremos na próxima seção.

2.3 ISO 27002

Enquanto a norma anterior tinha o foco no SGSI, esta norma foca principalmente na implementação e gerenciamento de controles, considerando os ambientes de riscos encontrados nas organizações.

> [a ISO 27002] fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização (ABNT, 2013b, p. 1).

A norma define que é essencial a identificação dos requisitos de segurança da informação, sendo eles vindo de três possíveis fontes (ABNT, 2013b). A primeira é por meio da avaliação de riscos, como apresentado na Unidade 1, na qual são levantadas as ameaças aos ativos de informação, suas vulnerabilidades, a probabilidade da ocorrência, que pode ser através da matriz de risco, e o potencial impacto ao negócio. A segunda é através da legislação vigente, como as definidas pelo Marco Civil da Internet, sobre o qual falaremos em breve, normas, estatutos, regulamentações e cláusulas contratuais. E a terceira é através de um conjunto de requisitos específicos da organização a fim de apoiar suas operações, como a categoria do empregado e os níveis de acesso à informação que ele possui, na qual um operário não deve ter acesso às informações da diretoria, por exemplo.

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles que incluem processos, políticas, dispositivos, práticas ou qualquer outra ação que modifica, preferencialmente reduz, um risco (ABNT, 2018b) e podem ser selecionados da própria ISO 27002. Esta seleção de controles depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco (diminuir, evitar, compartilhar ou reter o risco) e no enfoque geral da gestão de risco aplicado à organização.

Por exemplo, no âmbito de segurança em recursos humanos para a contratação de um profissional, um dos controles da norma ISO 27002 recomenda que sejam verificados alguns quesitos na etapa de seleção, antes mesmo da contratação. De qualquer forma, caso não esteja sendo feita nenhuma contratação, seria interessante seguir as diretrizes que o controle apresenta, para a equipe atual, como a confirmação das informações apresentadas no currículo, referências profissionais e pessoais, confirmação da qualificação, verificação de crédito e, inclusive, uma verificação de registros criminais, se a legislação permitir, é claro (ABNT, 2013b).

A ISO 27002 traz vários controles para implementar segurança da informação na organização e por mais que seja interessante aplicar todos eles, isto pode não ser vantajoso. Em Cazemier, Overbeek e Peters (2010, p. 21, tradução

nossa) é recomendado o que chamam de "segurança não mais que o necessário", que traz economia e simplicidade. Segundo os autores, a segurança além do necessário produzirá resultado oposto ao esperado, pois isso acaba fazendo com que as pessoas encontrem formas de driblar as regras, além de trazer uma sobrecarga de atividades e de tempo investida sem o retorno devido. O ponto a ser considerado é o foco nos riscos reais da organização, o qual pode ser feito, por exemplo, através da matriz de risco estudada na Unidade 1. Se tanto o impacto quanto a probabilidade forem baixos, não seria válido ele ter o mesmo investimento que algum que tenha um risco alto.

Uma consideração que a ISO 27002 traz é a respeito do ciclo de vida das informações e dos sistemas de informação. A informação passa desde a sua criação, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência (ABNT, 2013b).

Cada uma dessas etapas implica em um valor diferente para a informação. Consequentemente, níveis diferentes de segurança da informação precisam ser considerados em cada estágio (ABNT, 2013b). Por exemplo, o valor dos dados apresentados por um estudo sigiloso de viabilidade de um projeto será alto enquanto este projeto está nas suas primeiras etapas e, consequentemente, o investimento em segurança nessas etapas também deverá ser alto. Entretanto, quando o projeto já foi executado e aqueles dados já não forem mais sigilosos, o valor das informações será baixo, tal como a exigência de segurança necessária.

De forma similar, os sistemas de informação também possuem um ciclo de vida em que são concebidos, especificados, projetados, desenvolvidos, testados, implementado, usados, mantidos e, em alguns casos, retirados do serviço e descartados (ABNT, 2013b). Para esses sistemas, convém levar em consideração a segurança da informação em cada um destes estágios. As fases iniciais, por exemplo, sempre são excelentes oportunidades para atualizar e melhorar os controles de segurança, levando em consideração os incidentes acontecidos e riscos levantados.

O foco da norma em si são os controles de segurança da informação e suas respectivas diretrizes para implementação. No próximo tópico, veremos a respeito da PSI, e ao longo desta unidade, trataremos alguns exemplos de forma mais aprofundada. Leia a norma ISO 27002 (ABNT, 2013b) para maiores detalhes sobre cada um dos objetivos, controles e diretrizes para implementação.

Além da família ISO 27000 e de outras normas ISO, outras normas e padrões internacionais também abordam segurança da informação. Veremos um pouco sobre elas a seguir.

3 OUTRAS NORMAS E PADRÕES DE SEGURANÇA DA INFORMAÇÃO

Embora não sejam focados somente em segurança da informação, três grandes nomes fazem referência ao tema. São eles: COBIT (Objetivos de Controle de Informação e Tecnologia Relacionada), ITIL (Biblioteca de Infraestrutura de Tecnologia da Informação) e SOX (Lei Sarbanes-Oxley).

O COBIT é um padrão, também chamado de framework, para a governança e gestão de TI. Tem um caráter iterativo através do ciclo de vida de melhoria contínua e possui um modelo de capacidade de processo dividido em seis níveis, indo do zero, quando o processo não foi implementado ou não atingiu o objetivo ao nível 5, no qual o processo opera dentro dos limites definidos, produz resultado e é continuamente melhorado (ISACA, 2012).

O ciclo de vida de melhoria do COBIT acontece ao longo de sete fases. Na primeira é reconhecida e aceita a necessidade de implementação do COBIT. A segunda foca na definição dos objetivos de implementação, avaliando o estado atual, identificando os problemas e deficiências através da avaliação da capacidade do processo através do modelo comentado anteriormente (ISACA, 2012).

Na terceira fase, metas de melhoria de processo são definidas e analisadas. A próxima fase se concentra no planejamento de soluções práticas, que são implementadas na quinta fase. A sexta fase foca na operação e monitorização dos benefícios esperados, enquanto, na última fase, o sucesso é analisado globalmente e possivelmente novos requisitos são identificados, demonstrando a necessidade da melhoria contínua e dando início a um novo ciclo (ISACA, 2012).

Tal como o COBIT, a ITIL também é um conjunto de melhores práticas que está fortemente inserido no contexto da governança de TI e segurança da informação. Assim como também apresenta metas, atividades gerais, entradas e saídas de processos que podem ser incorporados na área de TI das organizações. De forma simplificada, enquanto o COBIT descreve **o quê**, a biblioteca ITIL descreve **como**, inclusive possibilitando que ambas sejam utilizadas em conjunto (SCHROEDER, 2016).

A ITIL possui um alto nível de flexibilidade e suas boas práticas são divididas em cinco volumes: Estratégia de Serviço, Desenho de Serviço, Transição de Serviço, Operação de Serviço e Melhoria Contínua do Serviço, sendo que

cada um deles possui processos que auxiliarão. O primeiro volume, Estratégia de Serviço, traz orientações para que a organização possa avaliar quais são os fatores que necessitam de melhoria e elabore um plano de direcionar as ações de TI (BUILDER, 2017).

O volume Desenho de Serviço demonstra como apresentar os protótipos que possibilitam a visualização daquilo que será desenvolvido para melhorar o fluxo de trabalho da TI, através do mapeamento de todos os requisitos que irão compor as soluções de TI.

O próximo volume, Transição de Serviço, orienta a respeito da implantação do serviço desenhado, assim como mudanças, e liberá-lo para utilização (BUILDER, 2017).

A Operação de Serviço visa gerir, com qualidade, outros aspectos que estão envolvidos no uso da TI, como acompanhar a performance do serviço e tratar as ocorrências. Por fim, o volume de Melhoria Contínua do Serviço visa a criação de mecanismos para avaliar constantemente os resultados obtidos com as modificações feitas, acompanhando, revisando e otimizando os serviços (BUILDER, 2017).

Enquanto as normas ISO, COBIT e ITIL foram criadas por entidades internacionais, o SOX teve uma origem diferente. Ela foi criada pelo congresso americano para proteger investidores contra fraudes americanas e tem influência global por definir responsabilidades para empresas de capital aberto que atuam no EUA.

Esta lei tem o intuito de garantir a transparência na gestão empresarial e reduzir riscos. Além de exigências, multas e outros detalhes, a lei incentivou as empresas a tornar seus relatórios mais eficientes, centralizados e automatizados (CAMARGO, 2017), consequentemente, incentivando a melhoria de seus sistemas de informação. E para atender a estes controles e demandas, a TI poderá utilizar frameworks, tais como a ISO 27001, COBIT e ITIL.

Confira mais sobre as normas e padrões de segurança da informação acessando os sites a seguir:

- COBIT – https://www.isaca.org/resources/cobit.
- ITIL – https://www.axelos.com/best-practice-solutions/itil.
- SOX – http://www.soxlaw.com/.

Além de normas e padrões internacionais de segurança da Informação, não é só o exterior que possui legislação nacional. Também existem leis que devem ser levadas em consideração aqui no Brasil, as quais veremos a seguir.

4 MARCO CIVIL DA INTERNET

Depois de vários anos sem uma legislação específica, com o poder judiciário buscando aplicar as leis do mundo físico no mundo virtual, em 23 de abril de 2014, foi sancionada a Lei nº 12.965/2014, também conhecida por Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (BRASIL, 2014).

Você sabia, por exemplo, que, segundo o Marco Civil da Internet, hoje a privacidade e a proteção dos seus dados na internet, incluindo seus e-mails e chats, só podem ser violadas em investigações criminais? Ou que se um cliente comete um crime virtual usando sua rede, seja ela uma Wi-Fi pública ou não, você responderá pelo crime? Ainda bem que Marco Civil da Internet também define como se proteger deste caso.

O Marco Civil da Internet reconhece para o ambiente virtual princípios constitucionais como a liberdade de expressão, a privacidade e os direitos humanos, além de definir responsabilidades dos provedores de serviços e orientar a atuação do Estado no desenvolvimento e uso da rede (BRASIL, 2014).

A Lei n° 12.965/2014 está baseada em três princípios: neutralidade, privacidade e liberdade de expressão (BRASIL, 2014). A neutralidade garante tratamento isonômico para qualquer pacote de dados, sem que o acesso ao conteúdo dependa do valor pago, ou seja, os provedores ficam proibidos de discriminar usuários com base nos serviços ou conteúdo que acessam. Por exemplo, não é permitido cobrar um valor para acessar e-mails ou proibir o acesso às plataformas de vídeos, como o YouTube.

A privacidade garante ao usuário o direito à inviolabilidade e ao sigilo das comunicações. As empresas deverão possuir mecanismos para garantir, por exemplo, que os e-mails só sejam lidos pelos emissores e pelos destinatários. Garante a proteção a dados pessoais e registros de conexão. E a cooperação das empresas de internet com órgãos de informação estrangeiros se torna ilegal.

Quanto à liberdade de expressão, a decisão sobre a retirada de conteúdos fica limitada à justiça. Antigamente vários provedores tiravam do ar textos, imagens e vídeos de páginas que hospedavam a partir de simples notificações, mas atualmente isso não é mais permitido.

Gostaria de conhecer o que mais a Lei n° 12.965/2014 estabelece? Acesse o endereço http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm e também esta matéria https://www.tecmundo.com.br/projeto-de-lei/42299-marco-civil-da-internet-o-guia-definitivo-do-projeto-de-lei.htm sobre ela.

O Marco Civil da Internet foi um grande passo para a segurança da informação no Brasil. Um outro importante marco legislativo foi a Lei Geral de Proteção de Dados (LGPD) que, dentre outras coisas, também legisla sobre a privacidade dos dados.

5 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Mais de 126 países no mundo possuem leis para a proteção de dados pessoais visando à regulamentação do tratamento de dados das empresas (SOARES, 2020) e o Brasil é um destes. Baseada na *General Data Protection Regulation* (GPDR) da União Europeia, em 14 de agosto de 2018, foi instituída a Lei nº 13.709/2018 (BRASIL, 2018), também conhecida como LGPD, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018, art. 1°).

O primeiro ponto a ser definido é o que são os dados pessoais. Segundo a LGPD, dado pessoal é, em síntese, qualquer informação que possa levar à identificação de uma pessoa, de maneira direta ou indireta. Exemplos: dados cadastrais (nome, CPF, endereço etc.), dados de GPS (*Global Positioning System*), identificadores eletrônicos, hábitos de consumo, preferências, entre outros (BLUM; LOPES, 2020). Com isso, ela tem uma enorme abrangência, abarcando tanto relações on-line quanto off-line. E o segundo ponto é a importância da privacidade, já estudado anteriormente, desses dados estarem definidos como um dos direitos fundamentais.

O tratamento desses dados pessoais precisa seguir dez princípios definidos no artigo 6º (BRASIL, 2018), sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Finalidade

Os dados devem ser tratados para determinados propósitos, os quais devem ser informados ao titular dos dados previamente, de modo explícito e sem que seja possível a utilização dos dados posteriormente para outra aplicação. "Quer dizer que se eu tenho os dados da pessoa para poder emitir a nota fiscal (hipótese de dispensa de pedido de autorização de coleta), eu não posso usar esses dados para enviar um e-mail marketing, ou uma publicidade?". Não. Não pode.

Adequação

Os dados devem ser usados de modo compatível com a finalidade declarada ao titular dos dados. "Isso quer dizer que se eu pedi os dados para mandar um newsletter e depois que quiser gerar um score para pesquisa qualitativa de algum produto, vou ter de pedir autorização de novo?". Sim, isso mesmo.

Necessidade

O tratamento deve ser limitado ao mínimo necessário para a realização do objetivo que você informou. Isso quer dizer que se o objetivo era conceder ou não um empréstimo no banco, todos os dados que não tenham relação com a posição creditícia – como gênero, orientação sexual, ideologia, filiação partidária ou sindical etc. – não devem ser tratadas ou conhecidas do operador de dados.

Livre acesso

Deve ser garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como o acesso à integralidade dos seus dados. Ênfase nos termos "facilitada", "gratuita" e "acesso à integralidade". Isso quer dizer que não serão aceitos formatos que o titular tenha de garimpar as informações, nem será possível cobrar pela compilação desses dados. Também será necessário entregar a totalidade dos dados que você possui. E tudo de graça.

Qualidade dos dados

Deve ser garantida a exatidão, clareza, relevância e atualização dos dados. Os dados entregues devem ser os que a empresa possui, não apenas os que foram coletados: os transformados também.

Transparência

Deve ser garantida a prestação de informações claras e facilmente acessíveis pelos titulares. Lembram do tormento que era o cancelamento de um serviço telefônico, por exemplo? A lei usa o princípio da Transparência para garantir que aquele calvário não ocorra. O titular deverá ser capaz de solicitar seus dados, de corrigi-los ou de solicitar sua exclusão de forma rápida, fácil e descomplicada.

Segurança

Deverão ser adotadas medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados. Aqui, temos um ponto importante, que deverá gerar o maior custo associado à nova lei. Além da responsabilidade pela adoção das medidas de proteção, a Autoridade Nacional de Proteção de Dados (ANPD) poderá dispor sobre os padrões técnicos mínimos aceitáveis.

Além disso, a lei introduz o conceito de *Privacy by Design* (PbD), que passa a ser obrigatório em processos de coleta de dados, armazenamento, transformação, circulação e uso dos dados. Também é importante salientar que o comando legal é dirigido não só ao campo técnico, mas também ao administrativo. Ou seja, pessoas e processos também serão responsáveis pelos dados e seu acesso ou processamento. A lei cria alguns novos atores, como o Controlador e o Operador de dados.

Prevenção

Deverão ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Notem que o princípio é de prevenção. Não bastará mais agir de modo reativo, ou seja, após o acidente. Se uma prevenção não for adequadamente implementada, os pressupostos jurídicos para uma ação de responsabilidade civil estarão postos: houve negligência, ou seja, descumprimento do dever geral de diligência (cuidado) a que todos estamos subordinados.

Não discriminação

Impossibilidade de tratamento para fins discriminatórios. Utilizar dados para fins que gerem discriminação são proibidos. O Direito da Antidiscriminação é um campo vasto e complexo, novo no Brasil.

A discriminação poderá ser direta ou indireta. Direta, quando a aplicação do processamento e seus resultados geraram um efeito negativo injustificável para alguém. Por exemplo, negar um empréstimo bancário com base na cor da

pele. Indireta, quando disposição, critério ou prática, aparentemente neutro, coloque pessoas de uma dada condição – racial ou étnica, por exemplo – em uma situação de desvantagem, comparativamente a outras pessoas.

Responsabilização e prestação de contas

As empresas deverão criar Controladores de dados, Operadores de dados e Encarregado de dados. Esses serão os responsáveis diretos por a empresa estar *compliance* com a nova lei. Além disso, a ANPD irá dispor sobre o relatório de impacto à proteção de dados pessoais, que as empresas deverão apresentar.

FONTE: <https://www.plugar.com.br/os-11-principios-e-a-aplicabilidade-da-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 5 ago. 2020.

Ainda existe um outro princípio, não descrito na LGPD, mas sim um princípio geral do Direito, chamado de boa-fé. Ele presume que as pessoas agem com boas intenções na realização dos negócios jurídicos e contrariá-lo gera um ônus jurídico, decorrente da quebra da boa-fé (PLUGAR, 2019). E ocorre, por exemplo, quando se diz que vai utilizar somente gênero, idade e renda, mas também utiliza nome e CPF.

Para o cidadão, a principal questão definida pela LGPD é o consentimento. Ela define que o titular do dado deve, quando quiser, autorizar de forma explícita e inequívoca que suas informações possam ser utilizadas, independente se por empresa ou órgão público, na hora que estiver usufruindo de um serviço ou produto, gratuito ou não. Assim, o consentimento será para finalidade determinada e clara. Por exemplo, sempre que você acessar o site para descobrir qual personagem da série Mr. Robot você é, ou qualquer outro quiz, fique muito atento a quais informações você está liberando. Isso pode facilitar muito, por exemplo, um ataque de engenharia social.

Você sabia que uma empresa varejista norte-americana descobre até gravidez de clientes com ajuda de software? Isso acontece porque ela armazena dados de seus clientes e faz uma análise e cruza dados na busca de padrões. Leia mais sobre o assunto no endereço: https://olhardigital.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231.

O importante é saber, também, que a LGPD garante ao titular dos dados pessoais o direito a obter do controlador várias informações e procedimentos (SERPRO, 2020). Para a análise dos direitos garantidos, considere um cenário hipotético, no qual você se cadastrou numa rede social há alguns anos, fornecendo vários dados, como seu nome completo, CPF, telefone celular, posição política e religião, mas os anos passaram, algumas informações mudaram, e aquele cadastro inicial ainda continua na rede social (TEIXEIRA, 2019).

A LGPD garante a confirmação de que existe um ou mais tratamento de dados sendo realizado, ou seja, você pode requisitar para a rede social se ela ainda mantém seu cadastro e se ela utiliza para algum fim. A lei também garante o acesso aos dados pessoais conservados que lhe digam respeito, ou seja, você pode requerer acesso aos seus dados de cadastro e qualquer outra informação capaz de te identificar, assim como deve ser possível corrigir os dados pessoais incompletos, inexatos ou desatualizados.

Também é permitido eliminar dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD, como, por exemplo, a eliminação do posicionamento político e religioso. Ou ainda revogar o consentimento de utilização e processamento das suas informações.

Para a operacionalização destas garantias, a LGPD define dois agentes de tratamento dos dados: o controlador e o operador. Ao primeiro compete as decisões referentes ao tratamento de dados pessoais. E o segundo realiza o tratamento de dados pessoais em nome do controlador.

Segundo Blum e Lopes (2020), as organizações, independente se no papel de controlador ou de operador, devem levar em consideração a LGPD, quanto aos dados pessoais de indivíduos localizados no Brasil, quando o tratamento se dá no Brasil e quando houver oferta de bens e serviços para indivíduos no Brasil. Por exemplo, não importa se o servidor de banco de dados está hospedado no exterior ou se a matriz da empresa está em outro país, se ela cumprir um dos três critérios mencionados anteriormente, deverá cumprir a LGPD.

Em contrapartida, a LGPD não se aplica para dados provenientes e destinados a outros países que apenas transitem pelo território nacional, para uso pessoal, para uso não comercial, com fins jornalísticos, acadêmicos e de segurança pública. Além de garantir os direitos dos usuários, também são obrigações das empresas: notificar em casos de incidentes de segurança envolvendo dados, seguir as regras específicas para tratar dados sensíveis, transferências internacionais e dados de crianças e adolescentes, e devem nomear um DPO.

O *Data Protection Officer* (DPO), conhecido também por Encarregado de Proteção de Dados, é a pessoa encarregada pelo tratamento de dados pessoais e é responsável, conforme a LGPD, por:

I- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II- receber comunicações da autoridade nacional e adotar providências;
III- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018, art. 41, § 2°).

RESUMO DO TÓPICO 1

Neste tópico, você aprendeu que:

- É importante, e recomendado, seguir um padrão internacional de segurança da informação.
- A principal família de normas internacionais de segurança da informação é a família ISO 27000, e suas correspondentes brasileiras definidas pela ABNT.
- A ISO 27000 apresenta as demais normas e define os termos utilizados.
- A ISO 27001 apresenta o SGSI que visa a garantia da confidencialidade, integridade e disponibilidade das informações da organização.
- Existem vários pontos a serem considerados para estabelecer, monitorar, manter e aprimorar o SGSI, assim como os principais benefícios com sua implementação, como redução de riscos e de custos.
- É importante utilizar o ciclo PDCA (*Plan - Do - Check - Act*) não somente para a segurança da informação, mas também expansível à outras situações.
- Os requisitos do SGSI para estar em conformidade com as recomendações internacionais são divididos em contexto da organização, liderança, planejamento, apoio, operação, avaliação de desempenho, melhoria.
- A ISO 27002 define os controles e diretrizes a serem implementados no SGSI para implementação da segurança da informação.
- O COBIT é um framework para a governança e gestão de TI.
- O ITIL é uma biblioteca de melhores práticas, divididas em cinco volumes: Estratégia de Serviço, Desenho de Serviço, Transição de Serviço, Operação de Serviço e Melhoria Contínua do Serviço.
- O Marco Civil da Internet é a principal lei brasileira que regulamenta tudo relacionado à Internet, centrada na neutralidade, privacidade, liberdade de expressão na rede.
- A principal lei brasileira, chamada de LGPD, é o que regulamenta tudo relacionado à proteção de dados, sejam eles pessoais ou da organização, que seguem os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

AUTOATIVIDADE

1 (DATAPREV, 2014 – Adaptado) Quando se trata de segurança da informação, devemos sempre nos preocupar com normas e procedimentos que a empresa vai seguir para suas atividades, a fim de proteger sua informação e a de seu cliente, haja que a informação é o bem mais precioso que se tem atualmente. Devemos levar em conta que muitas vezes lidamos com informações do cliente ou mesmo informações críticas da nossa empresa, que devem ter sua confidencialidade e integridade mantidas, e as normas agregam procedimentos que visam a essa segurança (embora seguir as normas não seja garantia total de segurança).

Considerando essa preocupação, a ISO criou a série 27000, com normas específicas de segurança, que são as mais usadas pelo mercado. A série ISO 27000 é composta por várias normas, uma das quais apresenta um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação. Identifique, a seguir, qual alternativa contém essa norma.

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/d61e85e4-fb>. Acesso em: 4 ago. 2020.

a) ( ) ISO 27001.
b) ( ) ISO 27002.
c) ( ) ISO 27003.
d) ( ) ISO 27004.

2 (TCM-GO, 2012 – Adaptado) A norma ISO27001 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Com relação ao monitoramento, a organização deve conduzir auditorias internas no SGSI a intervalos planejados para determinar se os objetivos de controle, controles, processos e procedimentos de seu SGSI:

I- Obedecem aos requisitos desta Norma e à legislação pertinente ou regulamentos.
II- São executados conforme esperado.
III- Obedecem aos requisitos de segurança da informação identificadas.
IV- São efetivamente implementados e mantidos.

Assinale a alternativa CORRETA:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/d61e85e4-fb>. Acesso em: 4 ago. 2020.

a) ( ) As afirmativas I, II, III e IV estão corretas.
b) ( ) As afirmativas I e IV estão corretas.
c) ( ) As afirmativas I, II e III estão corretas.
d) ( ) As afirmativas II, III e IV estão corretas.

3 (TCM-GO, 2012 – Adaptado) De acordo com a norma ISO27002, em Segurança de Recursos Humanos, antes do processo de contratação, convém que no processo de seleção sejam observados os seguintes itens:

I- Uma verificação das informações do curriculum vitae do candidato.
II- Confirmação das qualificações acadêmicas e profissionais.
III- Disponibilidade de referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal.
IV- Verificações financeiras ou de antecedentes criminais.

Assinale a alternativa CORRETA:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/8171c20c-b1>. Acesso em: 4 ago. 2020.

a) ( ) As afirmativas I, II, III e IV estão corretas.
b) ( ) As afirmativas I e IV estão corretas.
c) ( ) As afirmativas I, II e III estão corretas.
d) ( ) As afirmativas II e IV estão corretas.

4 (TJ-PA, 2014 – Adaptado)

O tempo dirá se o Marco Civil da internet é bom ou ruim

Foi aprovado o Marco Civil da internet: aquilo a que chamam de "Constituição da internet" e que será capaz de afetar diretamente a vida de milhões de usuários que já não usam mais a internet apenas para se divertir, mas para trabalhar.
O Marco Civil garantirá a neutralidade da rede, segundo a qual todo o conteúdo que trafega pela internet será tratado de forma igual. As empresas de telecomunicações que fornecem acesso poderão continuar vendendo velocidades diferentes. Mas terão de oferecer a conexão contratada independentemente do conteúdo acessado pelo internauta e não poderão vender pacotes restritos.
O Marco Civil garante a inviolabilidade e o sigilo das comunicações. O conteúdo poderá ser acessado apenas mediante ordem judicial. Na prática, as conversas via Skype e as mensagens salvas na conta de e-mail não poderão ser violadas, a menos que o Judiciário determine.
Excluiu-se do texto aprovado um artigo que obrigava empresas estrangeiras a instalar no Brasil seus datacenters (centros de dados para armazenamento de informações). Por outro lado, o projeto aprovado reforçou dispositivo que determina o cumprimento das leis brasileiras por parte de companhias internacionais, mesmo que não estejam instaladas no Brasil.

Ressalte-se ainda que a exclusão de conteúdo só poderá ser ordenada pela Justiça. Assim, não ficará mais a cargo dos provedores a decisão de manter ou remover informações e notícias polêmicas. Portanto, o usuário que se sentir ofendido por algum conteúdo no ambiente virtual terá de procurar a Justiça, e não as empresas que disponibilizam os dados.
Este é o Marco Civil que temos. Se é o que pretendíamos ter, o tempo vai mostrar. Mas, sem dúvida, será menos pior do que não termos marco civil nenhum.
(O Liberal, Editorial de 24.04.2014. Adaptado)

De acordo com o texto, o Marco Civil da internet:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/c4ac52ab-24>. Acesso em: 4 ago. 2020.

a) ( ) Dispõe sobre as relações entre empresas de telecomunicações e usuários da rede e defende o caráter inviolável dos conteúdos circulantes no ambiente virtual.
b) ( ) Garante que órgãos do governo tenham livre acesso a conversas via Skype e a mensagens salvas na conta de e-mail dos usuários brasileiros.
c) ( ) Determina quais conteúdos podem ser considerados neutros ou polêmicos, orientando os usuários quanto aos sites moralmente idôneos.
d) ( ) Exige que empresas estrangeiras instalem centros de armazenamento de dados e informações no Brasil se quiserem oferecer seus serviços a usuários brasileiros.

5 (CRN 3ª Região, 2019 – Adaptado) A Lei n° 13.709/2018 (Lei Geral de Proteção de Dados) incide quanto ao cadastro de usuários e clientes, alterando a maneira como as organizações devem tratar dados pessoais, com vistas a proteger os direitos fundamentais de liberdade e de privacidade e a respeitar o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania. Considerando o disposto na referida lei, assinale a alternativa CORRETA.

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/7019ffd7-7d>. Acesso em: 4 ago. 2020.

a) ( ) Essa lei aplica-se exclusivamente a dados coletados por meio digital.
b) ( ) O tratamento de dados pessoais, bem como o compartilhamento desses dados, somente é permitido mediante consentimento do titular, salvo casos de exceção previstos na lei.
c) ( ) Dados pessoais de crianças podem ser coletados sem consentimento prévio e armazenados para fins de contato com os pais ou o responsável legal.
d) ( ) O consentimento do tratamento dos dados deve ser fornecido pelo titular antecipadamente à coleta dos dados e presume concordância com o compartilhamento dos respectivos dados pessoais com entidades parceiras por tempo indeterminado.

6 (TJ-PA, 2020 – Adaptado) De acordo com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), as atividades de tratamento de dados pessoais devem observar a boa-fé e o princípio:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/0e34286c-44>. Acesso em: 4 ago. 2020.

a) ( ) De dado pessoal, segundo o qual a informação é relacionada à pessoa natural identificada ou identificável.
b) ( ) Da anonimização, com a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
c) ( ) Da prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
d) ( ) Da eliminação, que é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PLANO DE CONTINUIDADE DE NEGÓCIO

1 INTRODUÇÃO

Devido ao avanço da tecnologia, é cada vez maior o número de empresas que utiliza dos meios computacionais no seu dia a dia, seja para tarefas simples até aquelas que envolvem o núcleo do negócio. Consequentemente, cada vez mais as organizações se tornam dependentes de seus dados e das tecnologias envolvidas, exigindo atenção no quesito de segurança da informação.

Para Ferreira e Araújo (2008), uma organização que deseja ser bem-sucedida precisa ter um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações, e serviços, importantes recebam as devidas proteções, de modo que seja garantido sua confidencialidade, integridade e disponibilidade. A Política de Segurança da Informação (PSI) é um documento com a união deste conjunto de regras e padrões utilizados para a manutenção da segurança da informação.

Mas, o que acontece no caso de um desastre? Como a empresa se recuperaria? Para trabalhar neste cenário as organizações elaboram um outro documento chamado de Plano de Continuidade de Negócios (PCN), que tem como objetivo principal possibilitar o funcionamento da organização mesmo quando algo inesperado acontece.

Iniciaremos nossos estudos, neste tópico, primeiramente com a PSI, seguindo para a PCN no subtópico seguinte.

2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

Em geral, as empresas possuem regras quanto à segurança da informação. Seja um recepcionista que pede a identificação das pessoas, antes que entrem, ou mesmo a proibição de usar seu e-mail profissional para assuntos pessoais. Essas regras, e muitas outras, podem ser encontradas na PSI da organização.

A PSI é um conjunto de princípios que direcionam a gestão de segurança de informações e suas diretrizes determinam o que deve ser seguido pela organização para que sejam assegurados seus recursos computacionais e suas informações (TCU, 2012).

2.1 COMO ELABORAR UMA PSI

O conteúdo de uma PSI varia de organização para organização, pois cada uma é única, tem suas prioridades, processos e necessidades. Mas alguns temas normalmente são encontrados em todas elas. O primeiro e introdutório é um sumário executivo, com o propósito do documento, a definição de segurança da informação, os objetivos de segurança da informação para a organização e uma declaração do comprometimento da alta administração com a PSI, apoiando suas metas e princípios (TCU, 2012).

A PSI também deve conter a definição de responsabilidades gerais na gestão de segurança da informação, apresentando os cargos e suas responsabilidades. Precisa orientar sobre a análise e gerência de riscos, muito importantes para a correta prevenção de incidentes (TCU, 2012).

Sobre os sistemas, a PSI tem que apresentar os princípios de conformidade com a PSI e os padrões mínimos de qualidade que esse sistema necessita possuir (TCU, 2012). Por exemplo, se a PSI exige que para acessar um computador o usuário deve realizar um login, isso tem que estar descrito. Também é preciso descrever os procedimentos de prevenção e detecção de vírus, e intrusão, já apresentados na Unidade 2.

A PSI deve, também, apresentar alguns pontos sobre a legislação. Estes princípios legais precisam ser sempre observados quanto à TI, como direitos de propriedade de produção intelectual, direito sobre software, normas legais correlatas aos sistemas desenvolvidos e cláusulas contratuais, por exemplo (TCU, 2012). Assim como apresentar as consequências de violação das normas estabelecidas na PSI, como uma suspensão, demissão ou mesmo a abertura de um processo jurídico.

Além disso, existem temas que precisam ser abordados por uma PSI, mas que podem ser apresentados em documentos específicos, como, por exemplo, um documento que trata somente da política de backups. Nesses casos, a PSI referenciará estes outros documentos de políticas, ou então abordar, nela mesma, alguns temas específicos (ABNT, 2013b).

Além da política de backup, outras possíveis políticas e temas a serem abordados são de controle de acesso aos dados e ambientes da organização, segurança física e do ambiente, controles criptográficos para proteção, segurança nas comunicações e uma política de proteção e privacidade da informação de identificação pessoal. Alguns desses temas já foram estudados neste livro, e outros serão abordados, em detalhes, no Tópico 3.

Outro grande tema a ser abordado na PSI, ou numa política específica, são os tópicos orientados aos usuários finais das informações que estão sendo protegidas (funcionários, gestores, terceirizados etc.). Tais como uso aceitável

dos ativos, como os computadores da empresa, política de mesa limpa e tela limpa, dispositivos móveis e trabalho remoto e, também, restrições sobre o uso e instalação de software nos computadores e dispositivos da empresa.

Ao fim, a PSI é um dos requisitos básicos para a organização estar em conformidade com a LDPG e a ISO/IEC 27000, apresentadas no tópico anterior. A ISO 27002, mais especificamente, apresenta várias recomendações sobre os detalhes da PSI, sendo os principais apresentados na próxima seção.

2.2 PONTOS RELEVANTES PARA A IMPLANTAÇÃO

Na ICP-Brasil (infraestrutura que regulamenta toda a utilização de certificados digitais e assinatura digitais no Brasil), apresentada na Unidade 1 deste Livro Didático, a PSI elenca quatro requisitos de segurança: humano, físico, lógico e dos recursos criptográficos (ITI, 2019). O fator humano sempre deve ser considerado, inclusive para que este documento não seja engavetado e esquecido.

Para conhecer a Política Nacional de Segurança da Informação (PNSI) a nível federal, acesse: https://dsic.planalto.gov.br/pnsi/objetivo. E para conhecer o interessante Programa Nacional de Proteção do Conhecimento Sensível (PNPC), acesse: http://www.abin.gov.br/atuacao/programas/pnpc/.

Dentre esses aspectos humanos, Ferreira e Araújo (2008) recomendam que a PSI seja positiva e não apenas concentrada em ações proibitivas e punitivas, para que haja uma melhor aceitação das pessoas envolvidas, para que elas não se sintam proibidas com as restrições e sim beneficiadas com a segurança. Além disso, os autores reforçam que uma PSI tem que ser simples e escrita de maneira clara e precisa, ou seja, escrita da forma mais direta possível.

Além disso, as políticas de segurança da informação precisam ser criadas preferencialmente antes da ocorrência de algum incidente em segurança da informação, ou logo após a ocorrência de um, para que a brecha seja sanada. Segundo Hintzbergen *et al*. (2018), a PSI também necessita ser escrita em conformidade com os requisitos do negócio como, por exemplo, um site de e-commerce deve sempre verificar se o CPF possui restrições, bem como com as leis e os regulamentos relevantes, como considerar a LGPD no fornecimento de dados aos usuários.

Outro ponto relevante a ser considerado é que a PSI é elaborada e gerida normalmente por uma equipe de especialistas em segurança da informação. Entretanto, segundo Módulo (2020), a eficácia do processo de formalização, distribuição e controle das políticas, pode se transformar em um grande desafio para esta equipe pois é responsabilidade dela elaborar e gerir PSI, treinar as equipes de segurança da informação, disseminar para todas as partes interessadas e também garantir o cumprimento dos controles estabelecidos.

Uma determinada PSI é um documento que serve somente para a organização que a criou, pois possui muitas particularidades e, apesar de que todos dentro da organização devem conhecê-la, não é um tipo de documento que fica aberto publicamente para qualquer pessoa, pois pode apresentar informações sensíveis. Entretanto, algumas PSI são disponibilizadas, inclusive, na internet.

Uma PSI pública a ser analisada é o DOC-ICP-02 (ITI, 2019), que estabelece as diretrizes de segurança que serão adotadas pelas entidades participantes da ICP-Brasil. Ela define o que precisa ser feito, mas como isto será feito cabe somente à entidade. Por exemplo, ela define que "as responsabilidades pela segurança física dos sistemas das entidades deverão ser definidas e atribuídas a indivíduos claramente identificados na organização" (ITI, 2019, p.13), mas não determina quem, já que isto será uma particularidade da entidade.

> A política de segurança é um conjunto de documentos que devem ser destinados ao público correto para ser efetiva. Assim, diretrizes são para o público em geral, enquanto processos e procedimentos são específicos, como no caso do administrador do servidor de arquivos, que deve seguir o procedimento de configuração segura e rastreabilidade do serviço, por exemplo (NAKAMURA, 2016, p. 190).

O caso da ICP-Brasil é uma excelente fonte de exemplos de PSI e procedimentos de segurança da informação, pois ela é uma infraestrutura especialista em segurança e que possui diversos documentos, normas e procedimentos disponíveis de forma pública para consulta. No contraponto, lembre-se que, como apresentado na Unidade 1, segurança pela obscuridade não garante a segurança, mas isso não significa que todas as informações sejam expostas, mesmo porque privacidade é uma das principais propriedades de segurança da informação.

Por fim, é de conhecimento que a tecnologia muda e evolui todo dia e, desta forma, a PSI também deve refletir essas mudanças para que não fique obsoleta. E, para isso não acontecer, precisa passar por revisões, que dedicaremos um tópico exclusivo.

2.3 REVISÃO DA PSI

Como tudo que envolve pessoas, processos e tecnologias, deve passar por uma revisão crítica para que brechas sejam ajustadas, ou ainda para atualizar informações. A recomendação é que isso seja feito de forma planejada e periódica, ou, ainda, quando ocorrerem mudanças significativas como, por exemplo, a exigência de realização de auditoria, a fim de assegurar sua melhoria contínua. Além disso, é recomendado que exista um gestor que tenha a responsabilidade gerencial para o desenvolvimento, a revisão e para a avaliação de PSI (ABNT, 2013b).

Segundo Hintzbergen *et al*. (2018), a revisão tem que sempre incluir a avaliação de oportunidades de melhorias para a PSI, observando mudanças no ambiente da organização, mudanças nos negócios, nas legislações ou no ambiente técnico. Deve também levar em conta os resultados das revisões gerenciais e, antes de ser publicada, precisa passar pela aprovação da direção. Por fim, recomenda-se que, juntamente à PSI, o funcionário da organização assine um termo de responsabilidade (FERREIRA; ARAÚJO, 2008).

Para que uma organização tenha sucesso ao implementar a PSI, é necessário que exista um planejamento e uma estrutura adequada. Para isso, uma estrutura de gerenciamento tem que ser estabelecida para iniciar e controlar a implantação da segurança da informação dentro da organização. Entretanto, falhas e imprevistos acontecem e um plano de ação de emergência precisa existir.

3 PLANO DE CONTINUIDADE DO NEGÓCIO – PCN

O maior exemplo de imprevisto, nos tempos atuais, foi a quarentena causada pela COVID-19. Ela afetou a vida de milhões de pessoas e teve um enorme impacto na economia mundial (CUCOLO, 2020). Antes de um imprevisto acontecer, deve-se ter um planejamento prévio de como enfrentar e se reerguer para que as melhores decisões sejam tomadas. Este planejamento é conhecido como da Plano de Continuidade de Negócios (PCN): "PCN é o processo de gestão da capacidade de uma organização de conseguir manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de negócios críticos" (ABRAPP, 2012, p. 8).

Durante a epidemia, um dos principais documentos criados pelo Ministério da Saúde Brasileiro foi o *Plano de Contingência Nacional para Infecção Humana pelo novo Coronavírus COVID-19*, que norteou as ações do Ministério da Saúde na resposta à esta emergência de saúde pública. Um plano de contingência é uma das partes que o PCN deve tratar. Acesse o documento do Ministério da Saúde no endereço: https://portalarquivos2.saude.gov.br/images/pdf/2020/fevereiro/13/plano-contingencia-coronavirus-COVID19.pdf

Segundo Nakamura (2016), o foco principal da PCN está na propriedade de disponibilidade, estudado na Unidade 1, e visa a manutenção e o restabelecimento dos negócios após um incidente de segurança. Alguns desses incidentes podem ser causados por: desastres naturais, explosões, incêndios, fraudes financeiras, atentados, sabotagens, falhas nos sistemas informatizados ou nos equipamentos, queda da internet etc. E os planos de ação traçados precisam minimizar ou evitar os impactos negativos que possam ser causados, tais como: paralisações na produção e/ou prestação de serviços, perdas financeiras e danos à imagem ou credibilidade do negócio (POSITIVO TECNOLOGIA, 2017).

De acordo com Ferreira e Araújo (2008), as atividades relacionadas com o PCN devem estar integradas com a gestão de riscos do negócio e de TI, de forma que os riscos mapeados estejam parcialmente ou totalmente suportados pelo PCN. Na gestão de riscos, é feita uma análise utilizando a Matriz de Risco, estudada na Unidade 1, e seu propósito é identificar, de forma sistemática, quais incidentes podem ocorrer e, então, através do processo de tratamento de riscos, preparar a organização de forma a minimizar os danos de tais incidentes.

As duas principais normas a respeito de PCN são a ISO 22301, que trata do sistema de gestão de continuidade de negócios, de uma forma mais ampla, e a ISO 27031, que foca na continuidade dos negócios com enfoque na tecnologia da informação e comunicação. Assim como a ISO 27002, que apresenta, de forma sucinta, os controles e diretrizes para implantação de uma PCN.

Ghoddosi (2012) apresenta uma metodologia de gestão da continuidade do negócio, que consiste basicamente em seis passos: avaliação do projeto, análise de risco, análise de impacto nos negócios, desenvolvimento da PCN, treinamento e teste dos planos e, por fim, implementação e manutenção dos planos. O primeiro, avaliação do projeto, é o passo em que a organização deve definir o escopo e aplicabilidade do projeto, descrevendo o cenário em que se encontra, sua abrangência e suas limitações. O segundo passo é a análise de risco, já comentada anteriormente, quando é necessário identificar os riscos que ameaçam a continuidade dos processos da organização.

O terceiro passo de Ghoddosi (2012) é a análise de impacto nos negócios. É necessário estimar o impacto que a ocorrência de cada um dos desastres previstos poderá causar aos negócios/atividades da organização. Essa análise tem que quantificar o impacto financeiro, de imagem, operacional e legal, mapear os processos de negócio críticos e suas prioridades, além de mapear, também, as dependências internas e externas, recursos críticos e os prazos. Essa análise de impacto precisa responder, por exemplo, questões como qual o tempo de indisponibilidade que o negócio suporta.

O quarto passo de Ghoddosi (2012) é a elaboração da PCN em si, que veremos em mais detalhes na próxima seção. O quinto passo é a respeito de treinamento e teste dos planos. Esses planos devem ser testados constantemente, assim como os recursos destinados a estes, como já tido anteriormente, além de treinar todo o pessoal envolvido na implementação dos planos e validação dos procedimentos.

Por fim, o último passo que Ghoddosi (2012) descreve diz respeito à implementação e manutenção dos planos. Disponibilizar recursos materiais e humanos destinados aos planos, além das revisões periódicas para atualização do PCN frente à dinâmica dos processos da organização.

Que ver como o governo norte-americano coloca em prática seu plano de contingência quando o país é vítima de um ciber ataque? Assista ao filme *Duro de Matar 4.0* (2007), com Bruce Willis.

3.1 COMO ELABORAR UMA PCN

Dentre outras coisas, a PCN pode prever a elaboração e administração de planos específicos, como os Planos de Contingência Operacional (PCO), de Recuperação de Desastres (PRD) e de Gerenciamento de Crises (PGC).

Segundo a Abrapp (2012), o PCO é o plano que apresenta um conjunto de cenários de inoperância da organização e respectivos procedimentos alternativos, planejados para manter a continuidade das atividades prioritárias. O objetivo é reestabelecer o funcionamento dos serviços, por exemplo, depois de uma queda de conexão à internet.

Já o PRD aborda os cenários de desastre e os "respectivos procedimentos de reação para garantir que as atividades prioritárias retomem nível de operação aceitável dentro de prazo tolerável" (ABRAPP, 2012, p. 25). Ele determina o planejamento para que a empresa retome seus níveis originais de operação após o incidente.

E o PGC tem o foco em definir as funções e responsabilidades das equipes envolvidas antes, durante e após um incidente. Apresenta o "conjunto de cenários e os respectivos procedimentos de gestão para administrar, neutralizar ou eliminar impactos até a superação da crise" (ABRAPP, 2012, p. 25).

Esses três planos possuem focos diferentes e, mesmo que não sejam escritos em um documento específico para cada um, devem ser abordados na PCN, identificando os procedimentos e recursos necessários para eliminar ou reduzir o impacto.

Com as informações já levantadas até aqui, Magalhães e Pinheiro (2007) definem alguns pontos que a PCN deve cobrir. O primeiro deles é o sumário executivo, o qual apresenta o propósito do plano, autoridades e responsabilidades das pessoas principais, tipos de emergências que podem ocorrer e o local de gerenciamento da operação. O segundo ponto é o gerenciamento de elementos de emergência, descrevendo os processos de direção e controle, comunicação, recuperação, restauração, administração e logística.

A PCN precisa, também, apresentar os procedimentos de resposta à emergência, de preferência no formato de checklist, com as ações que devem ser tomadas. Também precisa apresentar documentos de suporte, tais como contatos das pessoas envolvidas, plantas das instalações físicas, guias com o mapeamento da infraestrutura de TI etc. E, por fim, também tem que conter uma lista de tarefas a serem executadas, definindo quem é o responsável, quando este deve agir e como tratar o problema encontrado (MAGALHÃES; PINHEIRO, 2007).

RESUMO DO TÓPICO 2

Neste tópico, você aprendeu que:

- A PSI é um conjunto de princípios que direcionam a gestão de segurança de informações na organização.
- Os vários pontos a serem considerados na elaboração de uma PSI são: a declaração da alta administração, definição de responsabilidades, os pontos relacionados à legislação e aos sistemas.
- As várias possibilidades de políticas específicas são: tela e mesa limpa, backup, e-mails e controle de acesso.
- A importância da definição, implantação e revisão periódica de uma política de segurança da informação dentro da organização, que, dentre outras características, deve ser simples e ter a aprovação da alta diretoria.
- Os principais tópicos a serem trabalhados na PSI são: criptografia, segurança física e controle de acesso.
- Os principais cuidados numa PSI são: estar em conformidade com as normas vigentes, ser do conhecimento de todos os trabalhadores e passar por revisões.
- O PCN está focado na garantia da propriedade de disponibilidade das informações.
- Há uma relação direta entre o PCN e a gestão de risco.
- Os seis passos para a elaboração do PCN são: avaliação do projeto, análise de risco, análise de impacto nos negócios, desenvolvimento da PCN, treinamento e teste dos planos e, implementação e manutenção dos planos.
- Os três subplanos do PCN são: Planos de Contingência Operacional (PCO), de Recuperação de Desastres (PRD) e de Gerenciamento de Crises (PGC).
- Os pontos que o PCN deve cobrir são: sumário executivo, gerenciamento de elementos de emergência, os procedimentos de resposta à emergência, os documentos de suporte e a lista de tarefas e seus responsáveis.

AUTOATIVIDADE

1 (UFG, 2010 – Adaptado) Existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido). Portanto, uma característica da política de segurança válida é a:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/eb5199a2-87>. Acesso em: 4 ago. 2020.

a) ( ) utilização, visto que o sistema deve ser utilizado de propósito geral com os objetivos determinados.
b) ( ) disponibilidade, esta característica deve estar disponível para quando o usuário necessitar utilizar os dados e solicitar ao administrador que mude as permissões de acesso.
c) ( ) integridade, pois o sistema deve estar sempre íntegro e em condições de ser usado, porém a senha tem de ser validada pelo gerente.
d) ( ) autenticidade, já que o sistema deve ter condições de verificar a identidade do usuário, e este deve ter condições de analisar a identidade do sistema.

2 (SUSEP, 2010 – Adaptado) Atualmente, a informação é um importante ativo para praticamente todo o tipo de organização. A segurança desse ativo faz-se necessária, seja por questão de conformidade com leis e contratos, seja para assegurar a continuidade do negócio. Por política de segurança entende-se:

FONTE: <https://www.questaocerta.com.br/questao/MjQ2NDc5>. Acesso em: 4 ago. 2020.

a) ( ) política planejada, válida para os setores críticos da organização, com regras o mais claro e simples possível, e estrutura gerencial de fiscalização dessa política, claramente sustentada pela alta hierarquia da área de informática.
b) ( ) política elaborada, implantada e em contínuo processo de revisão, válida para toda a organização, com regras o mais claro e simples possível, e estrutura gerencial e material de suporte a essa política, claramente sustentada pela alta hierarquia.
c) ( ) política e diretrizes de implantação, em contínuo processo de desenvolvimento, fiscalizada por toda a organização, com regras criptografadas e estrutura matricial e material de priorização dessa política, claramente sustentada pela alta hierarquia.
d) ( ) política elaborada, implantada e imune a revisões, válida para toda a organização, com estrutura gerencial de regras de formalização individualizada dessa política nas unidades organizacionais, claramente sustentada pelos gestores do nível operacional.

3 (CGU, 2004 – Adaptado) A política de segurança é um conjunto de diretrizes, normas, procedimentos e instruções de trabalho que estabelecem os critérios de segurança para serem adotados no nível local ou a institucional, visando o estabelecimento, a padronização e a normalização da segurança tanto no âmbito humano quanto tecnológico. Acerca da política de segurança da informação, analise as seguintes afirmações relativas a aspectos que devem ser considerados.

I- Uma boa política de segurança independe do treinamento aplicado aos funcionários.
II- A criptografia pode garantir a integridade dos dados e proteger informações sigilosas enviadas através de linhas inseguras.
III- Controle de acesso é aplicado após a implementação da política de segurança para garantir que todos os itens da política estão sendo cumpridos.
IV- A autenticação é como os usuários informam à infraestrutura de rede quem são eles.

Assinale a alternativa CORRETA:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/d904fd80-cb>. Acesso em: 4 ago. 2020.

a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas III e IV estão corretas.
c) ( ) As afirmativas I e III estão corretas.
d) ( ) As afirmativas II e IV estão corretas.

4 (VUNESP, 2018 – Adaptado) Considerando a segurança da informação em uma organização, dois importantes documentos a serem escritos e aplicados são a política de segurança da informação e o plano de continuidade de negócios. A respeito destes temas, é CORRETO afirmar que:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/9b00ded1-ea>. Acesso em: 4 ago. 2020.

a) ( ) A política de segurança da informação não inclui a forma de controle de acesso a seus equipamentos computacionais.
b) ( ) O propósito principal do plano de continuidade é a determinação dos horários de trabalho, sob condições normais, dos funcionários da empresa.
c) ( ) Um dos recursos necessários para que o plano de continuidade possa ser ativado inclui as pessoas ou recursos humanos.
d) ( ) Para a ativação do plano de continuidade, não é necessária a utilização de recursos tecnológicos.

5 (CCV-UFC, 2013 – Adaptado) Durante uma inspeção de rotina foi identificado que uma empresa não possui um plano de continuidade para um determinado serviço de TI. Escolha, entre as opções a seguir, qual seria um motivo válido para a inexistência do plano de continuidade para o serviço.

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/b090fb19-b6>. Acesso em: 4 ago. 2020.

a) ( ) A área de TI da empresa não possui competência para executar essa atividade.
b) ( ) Uma decisão foi tomada com base em uma avaliação dos impactos para o negócio.
c) ( ) Decidiu-se na área de TI da empresa que os riscos de problemas para esse serviço são reduzidos.
d) ( ) O service desk estaria preparado para resolver qualquer tipo de problema ou incidente sem o plano de continuidade para o serviço.

6 (DPE-RS, 2017 – Adaptado) O Plano de Continuidade dos Negócios é um roteiro de operações contínuas para quando as operações normais dos negócios são interrompidas por condições adversas. A respeito do Plano de Continuidade dos Negócios, assinale a alternativa CORRETA:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/70b16806-9e>. Acesso em: 4 ago. 2020.

a) ( ) Deve incluir, dentre outras coisas, a definição dos cenários de impacto e a análise de ameaças e riscos.
b) ( ) Deve ser de responsabilidade do departamento de TI, que é considerado o único com competências necessárias para conter possíveis desastres.
c) ( ) Deve possuir ações genéricas para conter qualquer tipo de desastre, evitando assim que tenha que ser revisado periodicamente.
d) ( ) Deve ser executado integralmente em resposta a incidentes que causem interrupção total ou parcial das operações normais de negócios.

TÓPICO 3

ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO E CONTROLE DE ACESSO

1 INTRODUÇÃO

Já foi apresentado em nosso estudo, na Unidade 1, que a segurança da informação deve ter como base três segmentos: pessoas, processos e tecnologias, sendo que já estudamos um pouco de cada um deles.

Além disso, para Sêmola (2013), a gestão da segurança da informação pode ser classificada em aspectos tecnológicos, físicos e humanos, sendo que, normalmente, as empresas possuem pelo menos alguma segurança em cada aspecto, nem que seja um antivírus, uma porta com chaves para que ninguém entre sem autorização ou algum folheto sobre a importância da segurança.

Além dos aspectos humanos relacionados à segurança da informação, que veremos logo a seguir, também veremos em breve outros tópicos relacionados ao tema, como os papéis que um colaborador possui e suas responsabilidades, assim como os cuidados que ele precisa ter ao utilizar dispositivos móveis e e-mails. Por fim estudaremos sobre controle de acesso.

2 ASPECTOS HUMANOS DA SEGURANAÇA DA INFORMAÇÃO

Quando se trata de segurança da informação, o fator humano sempre estará envolvido. Segundo Araújo, Araújo e Batista (2018), são atribuídas ao elemento humano diferentes tipos de vulnerabilidades relacionadas com os sistemas de informação. E quando essas pessoas se tornam alvo, por exemplo, de um ataque de engenharia social, o comprometimento da segurança torna-se iminente, independentemente das medidas protetivas (FRANGOPOULOS; ELOFF; VENTER, 2013).

Assista ao filme *Prenda-me se for capaz* (*Catch me if you can*) com o Leonardo DiCaprio e direção de Steven Spielberg. O filme é baseado na história real de Frank Abagnale, que utilizou de suas habilidades sociais de enganação para se passar como médico, advogado, copiloto, praticando golpes milionários e vivendo a vida como sempre quis.

Apesar da tecnologia fornecer diferentes meios para incrementar o nível de segurança da informação, existe a necessidade de mudar esses métodos de modo a incluir uma variável subjetiva: o fator humano (ARAÚJO; ARAÚJO; BATISTA, 2018). Em Carneiro e Almeida (2013) é apresentado um estudo sobre a percepção de segurança da informação do ponto de vista do usuário. Segundo esse estudo, os colaboradores em geral acreditam que todos na organização entendem o que é segurança da informação e conseguem identificar quais são as medidas de segurança da informação corporativa adotadas, mas ainda há dúvidas entre uma boa parte dos colaboradores sobre o seu próprio papel em segurança da informação, apesar de saberem identificar quem são os responsáveis pela segurança da informação na organização.

Continuando sobre o estudo de Carneiro e Almeida (2013), metade dos colaboradores acredita que segurança da informação é assunto apenas para os responsáveis pela tecnologia da informação. A grande maioria dos colaboradores têm a percepção de que a instituição investe mais em tecnologias do que em pessoas para garantir a segurança da informação, e acreditam que não há investimento suficiente na formação das pessoas no âmbito da segurança informacional.

Menos da metade dos colaboradores admitem conhecer e compreender políticas, procedimentos, normas e diretrizes de segurança da informação adotadas pela instituição e, paradoxalmente, a maioria afirma que se sente obrigado cumprir as políticas de segurança da informação instituídas, mesmo considerando que não as entendem (CARNEIRO; ALMEIDA 2013). Por fim, o estudo apresenta que a maioria dos colaboradores reporta a falta de um checklist para facilitar a orientação a respeito de segurança da informação.

Para sanar com as questões negativas do aspecto humano, assim como as já recomendadas pela PSI, pela LGPD e pela ISO 27002, recomenda-se as campanhas de divulgação e treinamento com todos envolvidos na organização. Outros pontos a serem considerados são apresentados a seguir.

3 PAPÉIS E RESPONSABILIDADES DA SEGURANÇA DA INFORMAÇÃO

Durante nosso estudo, foram citados alguns documentos a serem criados, como a PSI e a PCN, assim como várias atividades a serem realizadas, na maioria das vezes de forma periódica, por vários funcionários, cada um com seu papel (gestor, administrador, técnico etc.) e sua responsabilidade, como, por exemplo, o DPO descrito pela LGPD. Todos esses papéis e responsabilidades pela segurança da informação devem ser bem definidos e atribuídos, tais como a responsabilidade pela proteção de cada ativo, pelo cumprimento de processos de segurança da informação e pelas atividades de gerenciamento de riscos (ABNT, 2015).

Todos dentro de uma organização devem garantir a segurança da informação. Mas um dentre todos se responsabilizará e coordenará tudo relacionado. Este responsável pela segurança da informação pode ter vários nomes, dependendo de suas responsabilidades e das normas que a organização segue, como o DPO comentado anteriormente. A ANSI (*American National Standards Institute*) é o órgão norte americano similar à ABNT e define, por exemplo, o CSO (*Chief Security Officer*) (ANSI, 2013), também chamado de CISO (*Chief Information Security Officer*), um cargo similar ao tão conhecido CIO (*Chief Information Officer*), mas com foco em segurança da informação.

Segundo Sêmola (2013), o responsável pela segurança da informação é quem recebe toda a pressão da empresa diante dos resultados e quem é demandado a adequar o nível de controle e, portanto, o nível de segurança para suprir as novas demandas do negócio. Deve ser o mediador, orientador, questionador, analisador de ameaças, impactos e, consequentemente, responsável por um estudo de viabilidade para cada situação e etapas a serem impostas, na esfera das estratégias de análise dos riscos. Afinal, ele estará envolvido com os diversos setores da organização, receberá e emitirá opiniões sobre as atividades desenvolvidas e a forma de como assegurar a segurança das informações.

Conheça um pouco mais sobre o *Security Officer* em: https://www.profissionaisti.com.br/2013/07/o-papel-do-security-officer-agente-de-seguranca/.

Estes papéis e responsabilidades vão depender muito do porte da organização, assim como da preocupação com a segurança da informação. Alguns possíveis papéis são (ABNT, 2015):

- Alta Administração (DPO, CSO etc.): responsável pela visão, decisões estratégicas e pela coordenação de atividades para dirigir e controlar a organização.
- Diretor Executivo de Segurança da Informação: tem a responsabilidade e a governança globais em relação à segurança da informação, garantindo o correto tratamento dos ativos de informação.
- Segurança Física: é a pessoa responsável pela segurança física, por exemplo: das construções, e normalmente chamado de Gerente de Instalações.
- Gerência de Risco: a pessoa responsável pela estrutura de gerenciamento de risco da organização, incluindo avaliação de risco, tratamento de risco e monitoramento de risco.
- Auditor: é o responsável por avaliar o SGSI.

Essas responsabilidades devem estar bem documentadas e detalhadas na PSI para que o gestor responsável saiba o que cabe a ele fazer ou gerenciar (ABNT, 2013b). A respeito deste gestor, da mesma forma que ele tem que ser competente e capaz de cumprir com suas responsabilidades, a organização também precisa fornecer oportunidades de atualizá-lo com as melhores práticas através de cursos e formações (ABNT, 2013b).

Tudo isso tem que estar bem definido para uma boa gestão da segurança da informação. Definido os papéis e responsabilidades, outro ponto a ser estabelecido são as responsabilidades e cuidados ao se trabalhar fora da organização, trazer seus dispositivos para dentro da organização ou mesmo trabalhar utilizando dispositivos móveis, que serão descritos a seguir.

4 DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Nem sempre o colaborador trabalhará dentro da organização, com todas as proteções de segurança da informação garantidas por ela. Além disso, muitas vezes ainda será necessário tratar com informações sigilosas fora deste ambiente seguro, ou, ainda, o colaborador estará utilizando seu próprio dispositivo dentro do ambiente da empresa para tratar com essas informações.

Uma prática que está cada vez mais comum no mercado de trabalho brasileiro, já comum em países da Europa, é a BYOD (*Bring Your Own Device* – traga seu dispositivo). Nessa estratégia, o trabalhador utiliza seu computador pessoal para desenvolver as atividades na empresa. O uso do BYOD facilita tanto a mobilidade do empregador, no que se refere a recursos, bem como para quando há a necessidade de o funcionário realizar trabalhos em home office.

Com o uso expressivo dessa abordagem vem um questionamento, como garantir a segurança, tanto na perspectiva da empresa que libera recursos e acessos, bem como pela ótica do funcionário e do seu dispositivo?

Considerando esse cenário, a norma ISO 27002 (ABNT, 2013b) traz um bom detalhamento para a política de gerenciamento de riscos decorrentes do uso de dispositivos móveis e de trabalho remoto. A norma define que trabalho remoto é toda aquela forma de trabalho fora do ambiente da organização, incluindo ambientes de trabalho não tradicionais, como aqueles referidos como: ambientes de telecommuting, local de trabalho flexível, trabalho remoto, trabalho virtual ou teletrabalho.

Independentemente se utilizando dispositivos móveis ou realizando trabalho remoto, precisam ser tomadas as devidas precauções considerando os riscos de trabalhar em ambientes desprotegidos. Dessa forma, convém considerar, por exemplo, restrições quanto à instalação de softwares, controle de acesso e técnicas criptográficas. Nesses casos, o dispositivo estaria protegido, por exemplo, contra a instalação de um vírus, contra a tentativa de acesso quando o dispositivo está bloqueado e contra a leitura do SDcard, respectivamente.

Casos como uma simples perda, um furto ou mesmo um roubo, também devem ser considerados, já que é comum pessoas esquecerem seus celulares em taxis, ou similares, durante o trajeto a serviço da organização, principalmente quando esse dispositivo possui acesso a informações sensíveis do negócio. É melhor se prevenir, tendo em vista que com o número de um celular e as ferramentas certas, é possível realizar a clonagem de um celular se ele não estiver com as atualizações de segurança em dia, como demonstrou Mitnick em uma palestra da *Campus Party 2010* (LIMA, 2010).

Um ataque cada vez mais comum é através de estações de carregamento de bateria de aparelhos eletrônicos por USB, comuns em aeroportos e shoppings, por exemplo. Carregar nestes locais abre uma brecha para ataques de malwares instalados por hackers para roubar dados confidenciais sem autorização. Segundo Rodrigues (2019, s.p.) "conectar-se a um USB público é como encontrar uma escova de dentes na beira da estrada e decidir colocá-la na boca. Você não tem ideia de onde ou por onde essa coisa passou". É recomendado carregar o dispositivo em um local seguro, em um *power bank* ou, em último caso, manter o dispositivo desligado quando estiver carregando.

E relembrando um ponto essencial, para lidar com o aspecto humano é sempre importante lembrar a necessidade de treinamentos quanto ao risco adicional desta forma de trabalho. Em resumo, lidar com a segurança de dispositivos móveis, ou trabalho remoto, envolve as mesmas práticas de segurança utilizadas para dispositivos fixos, mas levando em consideração os riscos de estar fora das instalações da organização.

Quando considerando o trabalho remoto, além de algumas diretrizes comuns a respeito da utilização de dispositivos móveis, a política correspondente precisa levar em consideração os requisitos de segurança lógica, física e ambiental aplicável ao local do trabalho remoto para garantir das informações ali trafegando. Por exemplo, levar em consideração um método para acesso remoto seguro, a segurança física do local e até mesmo regras sobre o acesso de familiares e visitantes ao equipamento e às informações.

Muitas organizações restringem o acesso aos seus sistemas através do endereço IP de origem para garantir que somente um IP interno da organização consiga ter acesso. Quando o funcionário está fora do local do trabalho, ou ainda quando ele está em uma conexão de internet não segura, recomenda-se fazer uma VPN (*Virtual Private Network* – Rede Virtual Privada). Segundo Silva (2020), uma VPN permite acesso remoto a recursos de uma rede local, ainda que você não esteja fisicamente conectado nessa rede e, principalmente, serve para garantir proteção durante a troca de informações pela internet em redes públicas.

Um caso que muitas vezes ocorre no dia a dia, inclusive na utilização de dispositivos móveis, é o envio de mensagens eletrônicas, sejam e-mails, mensagens instantâneas ou outros, as quais exigem uma atenção especial, apresentada na próxima seção.

5 POLÍTICAS DE MENSAGENS ELETRÔNICAS

Fazendo trabalho remoto, ou mesmo presencial, muitas vezes será necessário o envio de mensagens eletrônicas, consequentemente, segundo a norma ISO 27002 (ABNT, 2013b), seria adequado que as informações que trafegam neste meio sejam devidamente protegidas. O desenvolvimento de uma PSI no emprego de mensagens eletrônicas no meio corporativo tem como objetivo proteger não somente os dispositivos, mas principalmente a informação em si.

Para isso acontecer, as mensagens tem que ser protegidas contra acesso não autorizado, modificação ou negação de serviço, assim, trazendo confiabilidade e disponibilidade. Um dos pontos a serem considerados são os controles e restrições quanto ao redirecionamento automático de mensagens eletrônicas para endereços externos, como o e-mail pessoal do funcionário, para que não haja vazamento de informação ou, ainda, deixar que uma informação sigilosa fique armazenada em um local possivelmente inseguro.

Quando utilizado em ambiente externo à organização, como redes públicas, deve haver um nível mais elevado de autenticação para controlar o acesso, é necessário, também, ter a aprovação prévia do superior, para utilizar tal serviço ou mesmo serviços públicos externos, como sistemas de mensagens eletrônicas, redes sociais ou compartilhamento de arquivos (ABNT, 2013b).

Nessa política deve-se, ainda, levar em consideração os aspectos legais como, por exemplo, requisito de assinaturas eletrônicas. No quesito legal, é importante ter em conta que a organização pode exercer de forma moderada, generalizada e impessoal, o controle de mensagens enviadas e recebidas por mensagem eletrônica corporativa (SILVEIRA, 2017), ou seja, ele pode ler seus e-mails.

Uma recomendação de segurança para acesso não somente ao seu e-mail, mas também a outros sistemas, é a utilização da autenticação em dois fatores. Além dessa recomendação, segue alguns outros exemplos de itens que muitas vezes são utilizados nas políticas de segurança de mensagens eletrônicas corporativas (AFROREGGAE, 2014):

- o serviço de e-mail deve ser destinado, exclusivamente, para atender aos interesses da instituição, sendo vedado seu uso para outros fins;
- deve ser vedada a realização de redirecionamentos para contas pessoais dos usuários;
- todas as informações produzidas ou recebidas pelos serviços de mensagens eletrônicas poderão ser acessadas a qualquer tempo pela instituição;
- os usuários deverão manter em sigilo sua senha de acesso ao e-mail, visto que esta senha é de uso pessoal e intransferível, realizando a substituição desta em caso de suspeita de violação;
- é vedada a utilização do serviço de e-mail para envio de materiais obscenos, ilegais, não éticos, pessoais, de propaganda ou de spam;
- é vedado transmitir ilegalmente propriedade intelectual da instituição ou de terceiros ou outros tipos de informações proprietárias sem a permissão do proprietário ou do licenciante;
- é vedado transmitir a terceiros o *mailing* (lista de todos os e-mails) da instituição.

Mesmo uma senha forte pode ser alvo de ataque, como aconteceu com o jornalista Mat Honan, que teve sua vida digital apagada quando um atacante se passou por ele, entrou em contato com a Apple e conseguiu a senha de acesso aos seus e-mails (ARRUDA, 2012). Mat conta que, além das falhas no processo de recuperação de senha da Apple, uma forma de ter evitado isso seria simplesmente ter utilizado a autenticação em dois fatores. Essa forma de autenticação, também conhecida por verificação em duas etapas, ou duas fases, é um método que exige não apenas algo que a pessoa saiba, como uma senha, mas também algo que possua, como seu smartphone (DONOHUE, 2014). Assim, um ataque que descobre a senha, como o ataque sofrido por Mat, ou mesmo um de força bruta, já não seria mais efetivo, pois exigiria a segunda confirmação.

É necessário ter uma atenção especial quando um mesmo e-mail é utilizado por mais de uma pessoa, como os e-mails comerciais. Uma forma é ter um controle de acesso com registro de qual dispositivo está acessando aquele e-mail.

6 CONTROLE DE ACESSO

Uma das formas para que um ataque seja bem-sucedido é ter acesso a determinadas informações confidenciais da organização, como uma simples senha, por exemplo. Para isso, existem as medidas de controle de acesso que, quando implementados de forma correta, permitem limitar o acesso a essas informações de forma equilibrada para que não haja nem poucas restrições, nem demais, mas na medida da necessidade da organização.

Veremos, a seguir, um pouco mais sobre controle de acesso, como os requisitos de negócio correspondentes, gestão de acesso e responsabilidades do usuário.

6.1 REQUISITOS DE NEGÓCIO PARA O CONTROLE DE ACESSO

Segundo Lento, Fraga e Lung (2006, p. 155), controle de acesso é um serviço de segurança que "limita as ações ou operações que um sujeito de um sistema computacional pode executar, restringindo o que ele pode fazer diretamente, como também os programas que podem ser executados em seu nome".

Para isso ocorrer, segundo a ISO 27002 (ABNT, 2013b), dois controles precisam ser implementados. O primeiro diz que os usuários devem receber acesso somente ao que são especificamente autorizados a usar, seja uma rede, um serviço ou qualquer outra forma de acesso à informação. E o segundo controle diz respeito a uma política de controle de acesso que seja desenvolvida, documentada e analisada.

Na legislação brasileira tudo é permitido, a menos que ela diga que aquele ato é proibido. Em uma boa política de segurança é utilizado a ideia oposta. Todo acesso precisa ser considerado proibido, a menos que seja expressamente permitido. É mais seguro, por exemplo, ter uma lista com todos os nomes de pessoas que podem entrar na empresa, do que ter uma lista com os milhares de nomes de pessoas que não podem entrar.

Segundo Teixeira Filho (2019), na política de controle de acesso considera-se o uso de controles de acesso físico e lógico de forma conjunta. Além disso, deve-se considerar a implantação de segregação de regras de controle de acesso,

por exemplo, pedido de acesso, autorização de acesso, administração de acesso. É preciso, também, considerar os requisitos para a autorização formal de pedidos de acesso e perfis de acesso de usuário na organização. Um dos pontos que surge é como fazer a gestão destes perfis e usuários.

6.2 GESTÃO DE ACESSO DO USUÁRIO

Para realizar este gerenciamento de forma correta, é necessário garantir que todo usuário autorizado tenha seu acesso liberado ao sistema e serviço requerido, assim como deve-se garantir que todo usuário não autorizado tenha esta requisição negada (ABNT, 2013b). Por garantia, nessa organização é necessário definir processos de distribuição de acessos que cubram todo o ciclo de vida deste acesso, desde a inscrição de um novo usuário até seu cancelamento. E dar uma atenção especial àqueles que possuem acessos privilegiados que permitem a criação ou liberação de acessos para outros usuários (TEIXEIRA FILHO, 2019).

A respeito dessa gestão de acessos, deve ser dado uma especial atenção também à imediata remoção ou desabilitação de usuários. Não pode ser possível que um funcionário demitido tenha seus acessos mantidos, pois, devido a vários motivos, não é incomum se revoltarem contra a empresa, levando dados corporativos, sequestrando dados ou fazendo vários outros ataques possíveis. Segundo artigo publicado no site da Access (ENTENDA, 2020), unir os setores de RH e da TI, mantendo uma comunicação direta entre ambos, pode sanar este e outros problemas, já que afetam todos os funcionários da empresa.

Um exemplo de funcionário demitido foi o caso de um administrador de sistemas que mudou as senhas principais de uma faculdade EAD norte-americana, deixando todos sem acesso aos sistemas e cobrando US$ 200 mil para informar a nova senha. Acesse https://olhardigital.com.br/fique_seguro/noticia/profissional-de-ti-pede-r-640-mil-para-resetar-uma-senha/65444 para mais detalhes.

Sobre o processo de distribuição de acessos, principalmente concessão e alteração, sempre leve em consideração a política de acesso, como descrito na seção sobre PSI, e demais requisitos (ABNT, 2013b). Por exemplo, verificar se aquele cargo pode ter acesso àquele sistema, se o superior dessa pessoa permite o acesso, assim como se o responsável pelo sistema também o permite. Também é recomendado que, por padrão, o usuário não tenha acesso, devendo o mesmo requerer o privilégio conforme a real necessidade.

Considerando essa necessidade comprovada, que o cargo/função permite e que a permissão do superior foi fornecida, ainda existem situações especiais em que é necessário um acesso privilegiado, como o de fornecedor de permissões, ou de super usuário em banco de dados ou sistema operacional. Nesses casos, além da atenção especial ao cumprimento das exigências, é recomendado, também, que exista uma autorização formal, seja estipulado um prazo de expiração e também que isto seja feito em um ID de usuário diferente do padrão para aquele usuário, para que funções privilegiadas não sejam feitas por contas normais, nem vice-versa (ABNT, 2013b).

Um caso de "excesso de confiança e falta de responsabilidade" foi quando 16,5 mil processos foram apagados do banco de dados do TCE-AM por servidores que não tomaram as devidas precauções".

FONTE: <https://canaltech.com.br/governo/funcionario-do-tce-am-executa-script-errado-no-sql-e-apaga-165-mil-processos-101596/>. Acesso em: 6 ago. 2020.

Independente do caso, antes do acesso ser liberado, todo usuário deve ter assinado uma declaração admitindo ter conhecimento dos seus direitos de acesso e dos seus deveres como usuário, incluindo possíveis sanções e punições. Esse usuário, então, é registrado com um identificador único e só então o usuário passará a usufruir de seus direitos de acesso (MACHADO, 2017).

E para garantir que está tudo conforme o previsto, deve haver uma análise do que está sendo feito, assim como revisar se as permissões condizem com as responsabilidades do usuário. Isso precisa ser feito de forma periódica e após qualquer tipo de mudança, como promoção ou rebaixamento, considerando que o intervalo para as permissões especiais deve ser menor do que a padrão.

6.3 RESPONSABILIDADES DO USUÁRIO

Como apresentado anteriormente, o termo assinado pelo usuário o responsabiliza pela proteção das informações/sistemas que ele tem permissão e, para isso, ele deve proteger principalmente suas informações de acesso, pois qualquer um que conseguir seu usuário e senha, por exemplo, poderá se passar por ele. Além de todas as recomendações apresentadas na Unidade 1, o usuário precisa ter consciência de que um controle de acesso efetivo depende também da proteção dos equipamentos, mídias de armazenamento e documentos utilizados por eles no ambiente de trabalho (MACHADO, 2017).

Para isso, por exemplo, o usuário deve bloquear seu equipamento quando não estiver em uso, cuidar com a impressão de informações sensíveis em impressoras compartilhadas, assim como cuidar ao transmitir esses documentos por dispositivos de armazenamento compartilhados, como uma pasta na rede, ou ainda tomar cuidado para não deixar informações sensíveis a mostra na mesa.

A ISO 27002 (ABNT, 2013b) recomenda a política de mesa limpa e tela limpa. Segundo Beal (2008), esta política visa reduzir os riscos de acesso não autorizado às informações corporativas, que se tornam mais vulneráveis quando papéis ou mídias removíveis são deixadas sobre a mesa e computadores são deixados ligados e conectados a sistemas ou redes na ausência do responsável. Entre as medidas de proteção sugeridas está a proteção de papéis e mídias em locais seguros quando não em uso, no bloqueio de equipamentos, no controle do uso de tecnologias fotocopiadoras (scanners e máquinas fotográficas, por exemplo) e em retirar imediatamente documentos sensíveis da impressora e de dispositivos e pastas públicas.

6.4 ACESSO A SISTEMAS E APLICAÇÕES

A proteção das informações de acesso, como comentado anteriormente, já previne diversos tipos de brechas de segurança, mas alguns outros pontos devem ser considerados no acesso a sistemas e aplicações para prevenir o acesso não autorizado aos sistemas e aplicações.

A ISO 27002 apresenta alguns controles que a serem implementados (ABNT, 2013b). Dentre eles, onde aplicável, o acesso tem que ser controlado por um procedimento seguro de entrada no sistema (log on), os sistemas para gerenciamento de senhas tem que ser interativos e assegurarem senhas de qualidade, o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações precisam ser restritos e estritamente controlados, assim como o acesso ao código-fonte de programas também deve ser restrito.

RESUMO DO TÓPICO 3

Neste tópico, você aprendeu que:

- É importante definir claramente os papéis e responsabilidades dos colaboradores da organização, assim como a definição de um CSO ou equivalente.
- As recomendações de cuidados para o tratamento de informações em dispositivos móveis e em trabalho remoto têm em vista as características de cada um deles.
- As principais recomendações a respeito de políticas de mensagens eletrônicas são os cuidados a serem tomados.
- As principais propriedades para um controle de acesso eficiente levam em consideração os usuários, recursos, operações, autoridade e domínio.
- A gestão do acesso de usuários às informações da organização deve seguir algumas recomendações, assim como a definição das responsabilidades de cada um.

AUTOATIVIDADE

1 (ESAF, 2008 – Adaptado) Segundo a ABNT NBR ISO/IEC 27002, segurança está fundamentada sobre três propriedades que devem ser mantidas: confidencialidade, integridade e disponibilidade das informações. Analise as afirmações relacionadas à segurança da informação e os objetivos do controle de acesso.

I- A disponibilidade é uma forma de controle de acesso que permite identificar os usuários legítimos da informação para que lhes possa ser liberado o acesso, quando solicitado.
II- A confidencialidade é uma forma de controle de acesso que evita que pessoas não autorizadas tenham acesso à informação para criá-la, destruí-la ou alterá-la indevidamente.
III- A integridade é uma forma de controle de acesso que evita o acesso de pessoas não autorizadas a informações confidenciais, salvaguardando segredos de negócios e protegendo a privacidade de dados pessoais.

Assinale a alternativa CORRETA:

FONTE: <https://www.tecnolegis.com/provas/comentarios/47825#:~:text=A%20integridade%20%C3%A9%20uma%20forma,a%20privacidade%20de%20dados%20pessoais.>. Acesso em: 4 ago. 2020.

a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas I e III estão corretas.
c) ( ) As afirmativas II e III estão corretas.
d) ( ) A afirmativa I está correta.

2 (CETESB, 2009 – Adaptado) O uso da VPN (Rede Privada Virtual) é uma necessidade nos dias de hoje para aumentar a segurança na comunicação de dados pela rede de computadores. A respeito do principal objetivo de uma VPN visa permitir, assinale a alternativa CORRETA:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/cdfb62de-9e>. Acesso em: 4 ago. 2020.

a) ( ) Utilizem IPs virtuais em uma rede local.
b) ( ) Realizem conexões remotas e seguras para redes corporativas.
c) ( ) Testem equipamentos e redes em ambiente de simulação.
d) ( ) Virtualizem os equipamentos utilizados na rede local.

3 (TRE-MS 2012 – Adaptado) Com base na norma NBR ISO/IEC 27.001:2013, o fato de uma organização manter computadores desligados ou com a tela travada quando estes não estiverem em uso e não manter papéis com senhas ou descrição de acesso a informações críticas em locais desprotegidos caracteriza a denominada "política de mesa limpa e tela protegida". A adoção dessa política tem um objetivo. Assinale a alternativa que corretamente apresenta este objetivo.

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/b9fc8db7-5b>. Acesso em: 4 ago. 2020.

a) ( ) Controle de gestão da continuidade do negócio.
b) ( ) Controle de gestão de incidentes de segurança da informação.
c) ( ) Controle de segurança de recursos humanos.
d) ( ) Controle de acessos.

4 (TJ-PA, 2020 – Adaptado) Um dos desafios atuais da segurança da informação é o crescente uso de BYOD (bring your own device, ou, em português, traga seu próprio dispositivo) nas instituições. Notebooks, tablets e principalmente smartphones estão invadindo as redes institucionais. Nesse contexto, são necessárias políticas, procedimentos e tecnologias especializadas acerca do tema. Com base na NBR ISO/IEC nº 27002, em uma política de dispositivos móveis, é CORRETO:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/0e6a83dc-44>. Acesso em: 4 ago. 2020.

a) ( ) Validar informações de entrada no sistema somente quando todos os dados de entrada estiverem completos e íntegros, em conformidade com as boas práticas.
b) ( ) Separar o uso do dispositivo para negócio e para fins pessoais, incluindo os softwares para apoiar essa separação e proteger os dados do negócio em um dispositivo privado.
c) ( ) Avaliar regularmente a referida política quanto a sua capacidade de atender ao crescimento do negócio e às interações com outras utilidades.
d) ( ) Segregar as funções de controle de acesso como, por exemplo, pedido de acesso, autorização de acesso e administração de acesso.

5 (TCE-RO, 2019 – Adaptado) Uma organização considera a possibilidade de implantar a modalidade de trabalho remoto, incluindo acesso remoto à intranet por meio de smartphones e computadores. Nessa hipótese, de acordo com a norma NBR ISO/IEC nº 27002:2013, recomenda-se:

I- Manter no campo de observação, os dispositivos móveis com acesso remoto autorizado que contenham informações importantes, sensíveis ou críticas para o negócio.
II- Usar criptografia nos dispositivos móveis e de acesso remoto, para prevenir o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos.
III- Fornecer acesso virtual às estações de trabalhos dos usuários com o objetivo de mitigar tentativas de ataques que venham a explorar falhas desse recurso.
IV- Acessar equipamentos de propriedade particular autorizados para acesso remoto, com o objetivo de verificar a segurança da máquina.

Assinale a alternativa CORRETA:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/9d8b1fe7-11>. Acesso em: 4 ago. 2020.

a) ( ) As afirmativas I, II e III estão corretas.
b) ( ) As afirmativas I e IV estão corretas.
c) ( ) As afirmativas I, II e IV estão corretas.
d) ( ) As afirmativas II, III e IV estão corretas.

AUDITORIA, SEGURANÇA FÍSICA E DO AMBIENTE

1 INTRODUÇÃO

Como visto anteriormente, a segurança da informação é baseada em confidencialidade, integridade e disponibilidade, sendo que qualquer vulnerabilidade que aconteça pode representar uma ameaça aos recursos da organização. Devido a isso, é interessante a aplicação de controles para garantir a integridade dos recursos envolvidos, sejam humanos ou tecnológicos. E uma das formas de aferir a conformidade é através de auditorias.

Historicamente, o termo auditoria foi inicialmente utilizado pelos ingleses para significar o conjunto de procedimentos técnicos para a revisão da contabilidade (MELO; SANTOS, 2017), mas na atualidade o termo não é utilizado somente para esta área. De forma mais genérica, auditoria se refere ao processo de examinar, corrigir ou certificar. Consiste em colocar determinada área ou processo da organização em análise, buscando entender como funcionam as atividades e quais são os problemas e possíveis melhorias a serem realizadas (GAEA, 2020). A seguir, veremos em mais detalhes como é realizado uma auditoria de sistemas.

2 AUDITORIA DE SISTEMAS

Segundo Fonseca (2012), a auditoria de sistemas de informação visa verificar o próprio ambiente informatizado, garantindo a integridade dos dados manipulados pelo computador. Ela estabelece e mantém procedimentos documentados para planejamento e utilização dos recursos computacionais da empresa, verificando aspectos de segurança e qualidade, já que ambas andam lado a lado. O trabalho da auditoria de sistemas acontece com o estabelecimento de metodologias, objetivos e procedimentos a serem adotados por todos aqueles que operam ou são responsáveis por equipamentos de TI e sistemas dentro da organização.

Numa auditoria é realizado o levantamento e análise de procedimentos e rotinas, com a função de oferecer a quem interessar (executivos, agentes públicos, acionistas etc.) uma posição neutra sobre sua adequação e que seja muito bem embasada em normas e princípios (LUZ, 2016). Independentemente do tipo de auditoria, que veremos em breve, é necessário conhecer o que delineará o processo de auditoria. É importante conhecer, por exemplo, as normas apresentadas no início desta Unidade, se sua organização pretende estar em conformidades com alguma delas, pois o auditor irá verificar cada ponto.

No que se refere à auditoria na família ISO 27000, as normas ISO 27006 e 27007 definem os requisitos e diretrizes para a auditoria de um SGSI, sendo que ambas referenciam e utilizam como base a ISO 19011 (ABNT, 2018a), que apresenta as diretrizes gerais para uma auditoria.

Os objetivos mencionados anteriormente são estabelecidos com base nas atividades da organização, seu tamanho, qualidade de seus sistemas e controle interno e competência de sua administração, demonstrando que cada auditoria é única. É necessário que o auditor tenha um modelo de como as atividades são feitas. Assim, leva-se em conta as atividades das pessoas, órgãos e produtos da organização de modo que tais atividades não se desviem das normas preestabelecidas (FONSECA, 2012)

Esses objetivos são metas a serem alcançadas, ou efeitos negativos a serem evitados, e são detalhados conforme o enfoque ao qual está relacionado (FONSECA, 2012). Conforme a ISO 19011, os objetivos podem ser baseados em vários critérios como considerando necessidades e expectativas das partes interessadas pertinentes; características e requisitos de processos, produtos, serviços e projetos; requisitos do SGSI; necessidade para avaliação de fornecedores externos e também baseados em resultados de auditorias anteriores (ABNT, 2018a).

A mesma norma, ISO 19011, exemplifica alguns objetivos de auditoria, que podem incluir a identificação de oportunidade para a melhoria; estar em conformidade com todos os requisitos pertinentes, como os para certificação em uma norma; determinar a contínua adequação, suficiência e eficácia do SGSI; avaliar a compatibilidade e o alinhamento dos objetivos do SGSI com a direção estratégica da organização, entre outros (ABNT, 2018a).

Gaea (2020) apresenta alguns benefícios relacionados à prática de auditorias de TI. Um deles é o aumento da eficiência do setor de TI, por abrir espaço para a utilização dos melhores processos e por garantir a solução dos principais problemas de TI por meio de planos de ação eficientes. A auditoria acaba alinhando as práticas de TI às exigências do mercado e às novidades na área, melhorando a gestão de TI, permitindo melhor entendimento sobre o funcionamento da área e acaba também aumentando a credibilidade do setor de TI, tanto perante os clientes quanto os outros setores da organização.

Esse aumento de eficiência também melhora o aproveitamento dos recursos existentes, tanto humanos quanto de equipamentos e de tecnologia, permitindo a redução dos custos da área e da empresa como um todo. Por fim, como todo o processo é estudado de forma mais aprofundada e então aprimorado, além de problemas solucionados, permite a neutralização e redução dos riscos.

Na literatura, há várias formas de se classificar uma auditoria. Por exemplo, a auditoria pode ser:

- quanto ao escopo (de processo, de produto ou de sistema de gestão) (CARDOSO, 2016);
- quanto à abordagem utilizada (ao redor do computador, baseada na confrontação de documentos com os resultados esperados; através do computador, envolvendo aprovação de registros de transações, manuseando o fluxo de dados; ou com o computador, utilizando técnicas de auditoria assistida por computador) (IMONIANA, 2017);
- quanto ao tipo da área envolvida (de programas do governo, contábil, administrativa, de legalidade etc.);
- quanto ao tipo de área da TI (integridade de dados, segurança da informação, segurança física, desenvolvimento etc.);
- ou mesmo quanto ao órgão fiscalizador (interna se feita pela própria organização, externa se feita por outra organização, ou articulada se feita por ambas) (CHIROLI, 2016).

Como o foco desta Unidade está nas normas e na consequente possibilidade de certificação, utilizaremos a categorização apresentada pela ISO 19011, a qual define três tipos: primeira parte, mais conhecida como auditoria interna; auditoria de segunda parte, também chamada de auditoria de fornecedor; e a auditoria de terceira parte, também chamada de auditoria independente ou externa (ABNT, 2018a).

A auditoria interna é aquela realizada por um departamento interno da organização e um dos objetivos é identificar quais itens não estão sendo atendidos, possibilitando a criação de plano de ação para ajustar os processos e assim se adequar à norma (ABNT, 2018a).

A auditoria de fornecedor são auditorias realizadas nos fornecedores da empresa, com o objetivo de atestar a capacidade dele em atender as necessidades e expectativas da empresa, podendo ser feita pela própria empresa ou por terceiros em seu nome (ABNT, 2018a).

E o terceiro tipo, a auditoria externa, é a auditoria realizada por uma entidade externa e independente da organização, com o objetivo de emitir um parecer sobre a adequação do SGSI quanto ao seu estabelecimento, documentação, implementação e manutenção, sendo um requisito necessário para a certificação (ABNT, 2018a).

O escopo da auditoria deve ser definido pelo responsável interno da auditoria e precisam compor um conjunto bem definido de pessoas, processos e tecnologias que correspondam claramente ao objetivo da auditoria. Mapear esses objetivos é um desafio para os auditores. Eles iniciam identificando a atividade de negócios com maior chance de produzir o melhor tipo de evidência para apoiar o objetivo da auditoria. Depois identificam quais sistemas e redes de aplicativos são usados para computar as informações que suportam as atividades operacionais e comerciais das companhias (TATICCA, 2020).

Na prática, o escopo da auditoria é mapeado conforme os objetivos definidos pelas partes interessadas, analisados e então o responsável pela auditoria coleta feedback dos membros do setor responsável e reúne evidências do que está sendo analisado. Ao final, a auditoria é documentada, de forma a deixar claro o passo a passo do processo, o cronograma de execução e os resultados encontrados. Além disso, são apresentados planos de ação para melhorias e correções na área de TI, baseados no processo de auditoria implementado dentro da empresa. (GAEA, 2020).

A ISACA (*Information Systems Audit and Control Association* – Associação de Auditoria e Controle de Sistemas de Informação), responsável pelo COBIT, já comentado anteriormente, desenvolve algumas certificações. Uma delas é a CISA (*Certified Information Systems Auditor*), uma das mais reconhecidas certificações do mundo, e requer conhecimento aprofundado, além de experiência profissional.

A auditoria sempre deve estar sincronizada com seus objetivos, como já mencionado anteriormente, e isso pode depender também do nicho de mercado que a organização se encontra. Por exemplo, a rigorosidade exigida no armazenamento de dados de uma software-house pode, em alguns casos, não ser a mesma aplicada à rigorosidade em um datacenter de um banco, que provavelmente estará dentro de uma sala-cofre, um tipo de área segura extremamente rigorosa.

3 ÁREAS SEGURAS

Dentro de uma organização, vários ambientes são utilizados para vários motivos, diversificando, desde os ambientes públicos, como uma recepção, a qual qualquer pessoa pode ter acesso, até áreas restritas, como o cofre de um banco. O objetivo destas áreas seguras é prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização (ABNT, 2013b). E, para tal, alguns controles deverão ser implementados:

- perímetros de segurança precisam ser definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis;
- áreas seguras têm que ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido, como o controle de acesso por PIN (*personal identification number*);
- projetar e aplicar segurança física para escritórios, salas e instalações, por exemplo, para evitar que informações confidenciais sejam visíveis e possam ser ouvidas da parte externa;
- projetar e aplicar proteção física contra desastres naturais, ataques maliciosos ou acidentes;
- projetar e aplicar procedimentos para o trabalho nestas áreas como, por exemplo, evitar trabalho não supervisionado;
- convém que pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

Este tema já foi apresentado e exemplificado na Unidade 1, cabendo a esta unidade apresentar as recomendações das normas internacionais.

Além de proteger as informações, como já estudado, e também proteger as áreas seguras, também é necessário proteger os equipamentos que armazenam as informações.

4 EQUIPAMENTO

O objetivo de proteger os equipamentos é impedir perdas, danos, furto ou roubo, ou comprometimento de informações ou ainda a interrupção das operações da organização (ABNT, 2013b). Para isso, a ISO 27002 (ABNT, 2013b) recomenda que:

- os equipamentos sejam colocados no local, ou protegidos, para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado;
- os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades, como suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, calefação/ventilação e ar-condicionado;
- o cabeamento de energia e de telecomunicações que transporta dado, ou dá suporte aos serviços de informações, seja protegido contra interceptação, interferência ou danos;
- os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente;
- equipamentos, informações ou software não sejam retirados do local sem autorização prévia;
- sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização, como já estudado na seção sobre trabalho remoto;
- todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos com segurança, antes do descarte ou do seu uso;
- os usuários assegurem que os equipamentos não monitorados tenham proteção adequada;
- e, como já apresentada anteriormente, a adoção de uma política de mesa limpa e tela limpa.

Além da proteção das informações, do equipamento que armazena/processa a informação e do local que guarda estes equipamentos, também é necessário a proteção durante o processamento sobre estes dados.

5 SEGURANÇA DAS OPERAÇÕES

Segundo a ISO 27002 (ABNT, 2013b), alguns pontos devem ser considerados na segurança das operações de armazenamento e processamento das informações.

O primeiro ponto é garantir a operação segura e correta dos recursos de processamento através da documentação dos procedimentos de operação; da gestão de mudanças quando houver algo que impacte na segurança da informação; através do monitoramento, ajuste as projeções na utilização dos recursos, independente de qual seja; e através da separação dos ambientes de desenvolvimento, testes e produção, principalmente como forma de reduzir os riscos de acesso ou modificações não autorizadas, além de ser uma boa prática de desenvolvimento (ABNT, 2013b).

O segundo ponto diz respeito à proteção contra códigos maliciosos, com a implementação de controles de detecção, prevenção e recuperação, combinado com um adequado programa de conscientização do usuário, como já estudado anteriormente (ABNT, 2013b).

O próximo ponto, também já abordado em nosso estudo, é a recomendação de proteção contra perda de dados (informações, softwares e imagens do sistema) através de backups (ABNT, 2013b). Observe que essas cópias de segurança devem ser efetuadas e testadas regularmente para que haja uma garantia em seu funcionamento.

Outro ponto importante na segurança das operações é o registro (log) de toda operação realizada, seja um evento de usuário, uma exceção ou mesmo uma falha. Esses logs devem ser produzidos, mantidos e analisados criticamente em intervalos regulares para a possível detecção de problemas operacionais, assim como de ataques (ABNT, 2013b).

Os logs requerem uma proteção maior para que não sejam lidos por pessoas não autorizadas, muito menos adulterados ou apagados. Se um atacante é bem-sucedido em alterar os logs, ele pode apagar todos seus rastros, dificultando ser detectado e consequentemente pego. É muito importante gerar evidências de tudo que ocorre no sistema, inclusive para facilitar o processo de auditoria (ABNT, 2013b).

Um dos casos que mobilizou boa parte dos investigadores de crimes cibernéticos da polícia federal foi quando o celular de um juiz federal foi alvo de ataque e todos os rastros foram apagados. Com isso, ministros da república, e vários outros cargos federais, passaram a utilizar celulares fornecidos pela ABIN. Mais informações em https://oglobo.globo.com/brasil/investigadores-estao-pessimistas-quanto-possibilidade-de-identificar-hacker-23735750.

Outro ponto a ser considerado é assegurar a integridade dos sistemas operacionais para que haja um controle nas instalações de softwares como forma de se proteger contra possíveis ataques. Somente usuário autorizado pode fazer uma nova instalação/atualização e, muitas vezes, isso ainda precisa de uma permissão superior, como no caso de instalações de softwares em servidores. E, por fim, deve-se prevenir a exploração de vulnerabilidades técnicas através da imediata avaliação e tomada de medidas apropriadas para lidar com os riscos associados (ABNT, 2013b).

LEITURA COMPLEMENTAR

9 PRINCIPAIS CERTIFICAÇÕES DE SEGURANÇA DE TI 2019

Charlotte Trueman

Elas ajudam a garantir que a equipe de TI tenha o conhecimento e as habilidades certas para detectar intrusos e impedir violações em geral

Uma das áreas de crescimento mais rápido das empresas é a de segurança cibernética. Todos os anos, mais ataques são realizados, significando que mais do orçamento de TI é alocado para reforçar a segurança, levando à necessidade de contratar mais especialistas em segurança cibernética para proteger a organização.

De acordo com a empresa de segurança cibernética CrowdStrike, que recentemente publicou um case book com dicas e insights sobre as linhas de frente dos casos de resposta a incidentes, as organizações não estão fazendo progressos substanciais para detectar intrusos e impedir violações em geral.

O estudo também descobriu que houve um aumento dramático no número de ataques que alavancaram a engenharia social e o phishing.

Com 82% dos profissionais de TI e de segurança cibernética alegando que eles não têm os talentos necessários em sua organização, CIOs e denais C-level deviam olhar com mais carinho para o treinamento de pessoal.

As certificações geralmente são a melhor maneira de garantir que as pessoas com quem você trabalha tenham o conhecimento e as habilidades certas para se destacar nessa tarefa. A Malásia chegou até mesmo a criar o seu próprio organismo de certificação que opera sob o 'Cybersecurity Malaysia Information Security Management System Audit and Certification (CSM27001)'. Ele fornece recomendações com base no Instituto Nacional de Padrões e Tecnologia (NIST) estrutura e desenvolveu um processo rigoroso para os fornecedores locais, que inclui uma avaliação completa de todas as qualificações.

Então, se você está contratando um novo funcionário ou procurando melhorar a qualificação de seus funcionários, aqui está uma lista de algumas das melhores certificações de segurança de TI atualmente em oferta.

1- CompTIA Security +

A CompTIA Security + é frequentemente considerada uma certificação básica, de nível básico, que pode funcionar como um trampolim para profissionais de TI que precisam assumir tarefas de segurança cibernética de nível intermediário.

Abrange segurança de rede, segurança de conformidade e operação, ameaças e vulnerabilidades, bem como aplicativos, dados e segurança do host.

- Custo: US $ 269.
- Requisitos: mínimo de dois anos de experiência em segurança de TI e rede.

2- GIAC Security Essentials (GSEC)

Esta certificação de nível de entrada é projetada para profissionais que procuram provar que possuem as habilidades e o conhecimento técnico necessários para ocupar funções de segurança "hands-on" além da compreensão de tecnologia e conceitos de segurança da informação.

Embora um programa de treinamento não seja essencial, os interessados em obter essa certificação podem considerar o curso do SANS GIAC, que inclui o custo do exame. A certificação GSEC deve ser renovada a cada quatro anos e pagar uma taxa de manutenção de US $ 429 no final de cada período.

- Custo: US $ 769, se parte do treinamento / bootcamp, US $ 1.899 (sem treinamento, também chamado de "desafio de certificação" ou "tentativa de certificação").
- Requisitos: nenhum treinamento específico é necessário, no entanto, a experiência prática é recomendada.

3- NIST Cybersecurity Framework (NCSF), Foundation e Practitioner

O curso NCSF do nível Foundation apresenta os candidatos ao NIST Cybersecurity Framework, descreve os atuais desafios da segurança cibernética e explica como as organizações que implementam um programa do NCSF podem atenuar esses obstáculos.

Já o do nível Practitioner fornece aos alunos as habilidades para projetar, construir, testar, gerenciar e melhorar um programa de segurança cibernética com base no NIST Cybersecurity Framework.

- Custo: US $ 995 para o Foundational, US $ 3.295 para o Practitioner
- Requisitos: o curso Foundational não tem pré-requisitos, mas você deve possuir uma Certificação NIST Cybersecurity Foundation válida ou ter conhecimento equivalente para concluir o Practitioner.

4- Offensive Security Certified Professional (OSCP)

O OSCP da Offensive Security é uma certificação ética de hacking destinada a profissionais de segurança da informação.

O curso ensina metodologias de teste de penetração e o uso das ferramentas incluídas na distribuição do Kali Linux. Requer que os titulares ataquem e penetrem com sucesso várias máquinas ativas em um ambiente de laboratório seguro.

É considerado mais técnico do que outras certificações de hacking ético e é uma das poucas certificações que exigem evidências de habilidades práticas de teste de penetração.

- Custo: a partir de US $ 800
- Requisitos: teste de penetração com o Kali Linux.

5- Certified Ethical Hacker (CEH)

Considerado um dos programas de treinamento em segurança da informação mais desejados em oferta atualmente, ele fornece aos alunos todas as habilidades necessárias para avaliar as fraquezas e vulnerabilidades dos sistemas e infraestruturas de TI.

Esta certificação é imprescindível para quem quer seguir uma carreira em testes de penetração ou hacking ético.

- Custo: US $ 500
- Requisitos: participar de um curso de treinamento aprovado pelo Conselho da CE de cinco dias ou ter pelo menos dois anos de experiência em segurança da informação.

6- Certified Information Security Manager (CISM)

Esta certificação é uma credencial de alto nível realizada por aqueles que procuram trabalhar no setor de segurança ou gerenciamento de risco.

Essa qualificação ensina toda uma gama de habilidades práticas de gerenciamento de segurança que são cruciais para qualquer profissional de segurança da informação.

- Custo: US $ 760
- Requisitos: cinco anos em segurança cibernética e três anos em gerenciamento de segurança.

7- Certified Cloud Security Professional (CCSP)

Uma certificação cada vez mais popular à medida que a computação em nuvem está em ascensão, o CCSP é projetado especificamente para profissionais de segurança da informação com ampla experiência em experiência em TI. É adequado para profissionais de nível médio a avançado envolvidos com segurança da informação, arquitetura de TI, governança, engenharia de segurança na Web e na nuvem, riscos e conformidade, bem como auditoria de TI.

Os detentores de credenciais do CCSP são competentes nos seis domínios do CCSP, ou seja, conceitos de arquitetura e requisitos de design, segurança de dados em nuvem, segurança de infraestrutura e plataforma em nuvem, segurança de aplicativos em nuvem, operações e conformidade legal.

- Custo: US $ 549 por tentativa.
- Requisito: um mínimo de 5 anos de tecnologia de informação cumulativa, paga e em tempo integral, incluindo pelo menos três anos de segurança da informação e um ano de computação em nuvem.

8- Certified Information Systems Security Professional (CISSP)

Outra certificação de alto nível, a CISSP é uma qualificação realizada por aqueles que trabalham em segurança de rede.

Fornecido pelo International Information Systems Security Certification Consortium, equipa os alunos com uma compreensão abrangente dessa área de conhecimento, incluindo segurança de ativos, engenharia e gerenciamento de acesso, para citar alguns.

- Custo: Um exame de seis horas a US $ 699 mais quatro exames de concentração adicionais de US $ 599 cada.
- Requisitos: Pelo menos 5 anos de experiência profissional recente em período integral em 2 ou mais dos 8 domínios do corpo de conhecimento comum do CISSP.

9- Certified Cloud Security Professional (CCSP)

Descrito como o "'gold standard" das certificações de segurança cibernética, essa qualificação de alto nível é muitas vezes procurada por organizações que desejam contratar um CISO.

Exige que os profissionais de gerenciamento de segurança demonstrem seu conhecimento sobre sete domínios-chave de segurança identificados pelos CPPs como as principais áreas envolvidas no gerenciamento de segurança.

- Custo: US $ 450
- Requisitos: Nove anos de experiência em segurança, pelo menos três dos quais responsáveis por uma função de segurança.

FONTE: <https://cio.com.br/9-principais-certificacoes-de-seguranca-de-ti-2019/>. Acesso em: 4 ago. 2020.

RESUMO DO TÓPICO 4

Neste tópico, você aprendeu que:

- É importante a preparação da organização para estar em conformidade com as normas e, consequentemente, estar preparada para o recebimento de auditorias.
- Uma auditoria realiza o levantamento e análise de procedimentos e rotinas da organização.
- Os objetivos da auditoria são metas a serem alcançadas, ou efeitos negativos a serem evitados.
- Os três principais tipos de auditoria são: de primeira parte (auditoria interna), de segunda parte (auditoria de fornecedor) e a de terceira parte (auditoria externa).
- A definição de perímetros de segurança, e seus respectivos controles, são importantes recomendações de segurança para áreas seguras.
- É importante proteger os equipamentos contra perdas, danos, furto ou roubo, ou comprometimento de informações ou ainda a interrupção das operações da organização.
- Os principais pontos a serem considerados na garantia da operação segura e correta dos recursos de processamento da informação são: documentação, proteção contra códigos maliciosos, proteção contra perda de dados, logs, integridade de sistemas operacionais e a prevenção contra a exploração de vulnerabilidades.

Ficou alguma dúvida? Construímos uma trilha de aprendizagem pensando em facilitar sua compreensão. Acesse o QR Code, que levará ao AVA, e veja as novidades que preparamos para seu estudo.

AUTOATIVIDADE

1 (TRE-AM, 2010 – Adaptado) Com relação à implementação de segurança em redes de computadores, considere:

I- No contexto empresarial, a segurança de redes é obtida através da utilização do uso apropriado de equipamentos e políticas de segurança que administrem o uso desses recursos em relação à segurança de redes e controle de acesso que assegurem a integridade dos serviços executados nos sistemas operacionais.
II- O entendimento apropriado sobre o risco permite aos administradores a habilidade de avaliar a relação custo-benefício e decidir sobre implementar controles para a correção de vulnerabilidades ou arcar com as consequências de uma ameaça potencial de invasão.
III- Em ambientes de rede de computadores o gerenciamento de riscos deve ocorrer através de auditorias periódicas nos principais equipamentos de conectividade e sistemas de proteção de rede existentes. O processo de análise de riscos deve cobrir o maior número possível de ativos de tecnologia, tais como: roteadores de borda, roteadores de acesso remoto, access points, sistemas de proxy, sistemas antivírus e firewalls.
IV- O custo para implementar controles que evitem vulnerabilidades, tais como: servidores de e-mails inadequadamente configurados, implementações de segurança específicas para alguns ativos de TI e substituição de servidores open relay é relativamente maior que suas consequências, invalidando, dessa forma, a política de segurança.

Assinale a alternativa CORRETA:

FONTE: <https://olhonavaga.com.br/questoes/questoes?id=388615&tc=1>. Acesso em: 4 ago. 2020.

a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas I e IV estão corretas.
c) ( ) As afirmativas I, II e III estão corretas.
d) ( ) As afirmativas II, III e IV estão corretas.

2 (TRE-MS, 2012 – Adaptado) Para proteger uma área que abriga recursos de processamento da informação, um órgão público, com base na norma ABNT NBR ISO/IEC 27001, instalou uma porta com controle de acesso por cartão, de modo a que somente os colaboradores previamente autorizados possam acessar esse ambiente. Nessa situação hipotética, de acordo com a referida norma da ABNT, assinale a medida adotada pelo órgão público a que se associa.

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/b89d20c8-5b>. Acesso em: 4 ago. 2020.

a) ( ) À validação de dados de saída.
b) ( ) Ao controle de vulnerabilidades.
c) ( ) Ao controle contra códigos móveis.
d) ( ) Ao controle de perímetro de segurança física.

3 (CGU, 2004 – Adaptado) Considere um sistema no qual existe um conjunto de informações disponível para um determinado grupo de usuários denominados "auditores". Após várias consultas com respostas corretas, em um determinado momento, um usuário pertencente ao grupo “auditores” acessa o sistema em busca de uma informação e recebe, como resposta a sua consulta, uma informação completamente diferente da desejada. Nesse caso, houve uma falha na segurança da informação para este sistema. Assinale a alternativa que apresenta a propriedade relacionada à falha.

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/ba82933c-9a>. Acesso em: 4 ago. 2020.

a) ( ) Confidencialidade.
b) ( ) Integridade.
c) ( ) Auditoria.
d) ( ) Privacidade.

4 (CGU, 2006 – Adaptado) De acordo com a norma ABNT NBR ISO/IEC 27001 de 2013, a organização deve conduzir auditorias do SGSI. Analise as seguintes afirmações relacionadas a Auditoria de Sistemas.

I- O auditor de Tecnologia da Informação deve ser ligado diretamente à área sob auditoria, devendo ser, preferencialmente, um funcionário ou ter um cargo nessa área.
II- O colaborador a ser auditado deve planejar as tarefas de auditoria para direcionar os objetivos da auditoria e seguir os padrões profissionais aplicáveis.
III- O auditor de Tecnologia da Informação deve requisitar e avaliar informações apropriadas sobre pontos, conclusões e recomendações anteriores e relevantes para determinar se ações apropriadas foram implementadas em tempo hábil.
IV- A auditoria realizada em Tecnologia da Informação engloba a verificação de operações, processos, sistemas e responsabilidades.

Assinale a alternativa CORRETA:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/5583467b-f6>. Acesso em: 4 ago. 2020.

a) ( ) As afirmativas I e II estão corretas.
b) ( ) As afirmativas II e III estão corretas.
c) ( ) As afirmativas III e IV estão corretas.
d) ( ) As afirmativas I e IV estão corretas.

5 (DPE-RJ, 2019 – Adaptado) De acordo com a norma ABNT NBR ISO/IEC 27001:2013, uma organização deve programar auditorias internas a fim de verificar a aderência da conformidade do sistema de gestão da segurança da informação aos seus requisitos e à legislação vigente. Sobre a realização da auditoria interna, é correto afirmar que:

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/f6b927aa-65>. Acesso em: 4 ago. 2020.

a) ( ) Os critérios de verificação devem ser sempre os mesmos, independentemente do escopo ou do processo da organização a ser auditado.
b) ( ) Os auditores não devem conhecer e considerar os resultados das auditorias anteriores para não influenciarem o trabalho de verificação.
c) ( ) Os auditores devem ser do próprio setor auditado a fim de possibilitar o aproveitamento de seu conhecimento acerca das atividades desenvolvidas.
d) ( ) Os resultados das auditorias devem ser de conhecimento da direção responsável pelo setor auditado.

6 (SEFAZ-SP, 2013 – Adaptado) A auditoria da segurança da informação avalia a política de segurança e os controles relacionados adotados em cada organização. Nesse contexto, muitas vezes, as organizações não se preocupam, ou até negligenciam, um aspecto básico da segurança que é a localização dos equipamentos que podem facilitar a intrusão. Na auditoria de segurança da informação, assinale a alternativa que apresenta o nome desse aspecto.

FONTE: <https://www.qconcursos.com/questoes-de-concursos/questoes/6e45c0db-ee>. Acesso em: 4 ago. 2020.

a) ( ) Controle de acesso lógico.
b) ( ) Controle de acesso físico.
c) ( ) Controle de conteúdo.
d) ( ) Controle de entrada e saída de dados.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 19011**: tecnologia da informação - técnicas de segurança - sistema de gestão da segurança da informação - visão geral e vocabulário. Rio de Janeiro: ABNT, 2018a.

ABNT. **NBR ISO/IEC 27000**: tecnologia da informação - técnicas de segurança - sistema de gestão da segurança da informação - visão geral e vocabulário. Rio de Janeiro: ABNT, 2018b.

ABNT. **NBR ISO/IEC 27003**: tecnologia da informação - técnicas de segurança - diretrizes para implantação de um sistema de gestão da segurança da informação. Rio de Janeiro: ABNT, 2015.

ABNT. **NBR ISO/IEC 27001**: tecnologia da informação - técnicas de segurança - sistema de gestão da segurança da informação - requisitos. Rio de Janeiro: ABNT, 2013a.

ABNT. **NBR ISO/IEC 27002**: tecnologia da informação - técnicas de segurança - técnicas de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013b.

ABRAPP, Comissão Técnica Regional Sudeste de Governança da. **Guia de boas práticas para planos de continuidade de negócios**. São Paulo: ABRAPP, 2012. Disponível em: http://www.abrapp.org.br/GuiasManuais/guia_continuidade_negocios.pdf. Acesso em: 1° maio 2020.

AFROREGGAE. **Comunicado 1, de 13 de janeiro de 2014**. **Política de privacidade para e-mail institucional, celular corporativo e computadores**. Rio de Janeiro: Grupo Cultural AfroReggae, 2014. Disponível em: https://www.afroreggae.org/wp-content/uploads/2014/05/comunicado-politica-de-privacidade-para-email.pdf. Acesso em: 1° abr. 2020.

ANSI. **ANSI/ASIS CSO.1-2013**: chief security officer - an organizational model. x: asis international, Washington, D.C.: ANSI, 2013. 32 p.

ARAÚJO, W. J. de; ARAÚJO, S. G. L.; BATISTA, R. R. Estudo dos aspectos humanos da segurança da informação aplicado na Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba - UFPB. **Informação & Informação**, Londrina, v. 23, n. 2, p. 596-618, maio/ago. 2018. Disponível em: http://dx.doi.org/10.5433/1981-8920.2018v23n2p596. Acesso em: 5 ago. 2020.

ARRUDA, F. **Saiba como hackers apagaram a vida digital de um jornalista em apenas uma hora. Tecmundo**, São Paulo, 7 ago. 2012. Disponível em: https://www.tecmundo.com.br/seguranca/27993-saiba-como-hackers-apagaram-a-vida-digital-de-um-jornalista-em-apenas-uma-hora.htm. Acesso em: 1° abr. 2020.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BLUM, R. O.; LOPES, N. Lei geral de proteção de dados no setor público: transparência e fortalecimento do estado democrático de direito. **Cadernos Jurídicos (EPM)**, São Paulo, ano 21, n. 53, p. 171-178, mar. 2020. Disponível em: http://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_7_cadernos_juridicos_epm.pdf?d=637250348268501368. Acesso em: 25 ago. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Poder Executivo, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 mar. 2020.

BRASIL. **Lei nº 12.965, de 25 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília: Poder Executivo, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1 mar. 2020.

BUILDER, P. **O que é ITIL e o como ele se encaixa na área de TI da sua empresa**. 30 maio 2017. Disponível em: https://www.projectbuilder.com.br/blog/o-que-e-itil-e-o-como-ele-se-encaixa-na-area-de-ti-da-sua-empresa/. Acesso em: 1° jul. 2020.

CAMARGO, R. F. de. Lei Sarbanes-Oxley: aprimorando a prestação de contas com a SOx. **Treasy**, Joinville, 22 maio 2017. Disponível em: https://www.treasy.com.br/blog/sox-lei-sarbanes-oxley/. Acesso em: 1° jul. 2020.

CARDOSO, A. (org.). **Auditoria de sistema de gestão integrada**. São Paulo: Pearson, 2016. 132p.

CARNEIRO, L. E. dos S.; ALMEIDA, M. B. Segurança da informação: uma investigação na perspectiva do usuário de sistemas de informação corporativos em uma organização de saúde. *In*: CONFERÊNCIA IBERO AMERICANA COMPUTAÇÃO APLICADA, 2013, Porto Alegre. **Anais** [...]. Porto Alegre: IADIS, 2013. p. 127-134. Disponível em: http://mba.eci.ufmg.br/downloads/IADIS%20Conference%20Seg%20Inform%20camera%20ready%20web.pdf. Acesso em: 1° abr. 2020.

CAZEMIER, J. A.; OVERBEEK, P.; PETERS, L. **Information security management with ITIL V3**. 's-Hertogenbosch: Van Haren Publishing, 2010. 132 p.

CHIROLI, D. M. de G. **Avaliação de sistemas de qualidade**. Curitiba: InterSaberes, 2016. 308 p.

CUCOLO, E. Dados mostram a dimensão histórica do impacto da Covid-19 na economia. **Folha de São Paulo**, São Paulo, 11 jul. 2020. Disponível em: https://www1.folha.uol.com.br/mercado/2020/07/dados-mostram-a-dimensao-historica-do-impacto-da-covid-19-na-economia.shtml. Acesso em: 15 jul. 2020.

DONOHUE, B. O que é a autenticação de dois fatores e como usá-la? **Kaspersky daily**, [*s. l.*], 2014. Disponível em: https://www.kaspersky.com.br/blog/o-que-e-a-autenticacao-de-dois-fatores-e-como-usa-la/3226/. Acesso em: 1° jul. 2020.

ENTENDA as vantagens de unir o RH e a TI para a segurança dos documentos. **Access**, São Paulo, c2020. Disponível em: https://www.accesscorp.com.br/entenda-as-vantagens-de-unir-o-rh-e-a-ti-para-a-seguranca-dos-documentos/. Acesso em: 22 ago. 2020.

FARIA, C. PDCA (plan, do, check, action). **InfoEscola**, [*s. l.*], c2020. Disponível em: https://www.infoescola.com/administracao_/pdca-plan-do-check-action/. Acesso em: 1° abr. 2020.

FERREIRA, F. N. F.; ARAÚJO, M. T. de. **Política de segurança da informação**: guia prático para elaboração e implementação. 2. ed. rev. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

FONSECA, G. Auditoria de sistemas de informação: conheça mais sobre o assunto. **Profissionais TI**, [*s. l.*], 19 abr. 2012. Disponível em: https://www.profissionaisti.com.br/2012/04/auditoria-de-sistemas-de-informacao-conheca-mais-sobre-o-assunto/. Acesso em: 1° abr. 2020.

FRANGOPOULOS, E. D.; ELOFF, M. M.; VENTER, L. M. Psychosocial risks. **Information Management & Computer Security**, Melbourne, v. 21, n. 1, p. 53-65, 15 mar. 2013. Disponível em: http://dx.doi.org/10.1108/09685221311314428. Acesso em: 5 ago. 2020.

GAEA. Auditoria de TI: tudo o que você precisa saber sobre o assunto! **Gaea**, [*s. l.*], c2020. Disponível em: https://gaea.com.br/auditoria-de-ti-tudo-o-que-voce-precisa-saber-sobre-o-assunto/. Acesso em: 1° abr. 2020.

GHODDOSI, N. **Gestão da segurança da informação**. Indaial: UNIASSELVI, 2012. 102 p.

HINTZBERGEN, J. *et al*. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. 267 p.

IMONIANA, J. O. **Auditoria de sistemas de informação**. 3. ed. São Paulo: Atlas, 2017. 197 p.

PLUGAR. Os 11 princípios e a aplicabilidade da Lei Geral de Proteção de Dados (LGPD). **Plugar data & Intelligence**, Porto Alegre, 28 mar. 2019. Disponível em: https://www.plugar.com.br/os-11-principios-e-a-aplicabilidade-da-lei-geral-de-protecao-de-dados-lgpd/. Acesso em: 1° abr. 2020.

ISACA. **COBIT 5**: modelo corporativo para governança e gestão de TI da organização. Rolling Meadows: ISACA, 2012. 98 p.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Política de segurança da ICP-Brasil**: DOC-ICP-02 -versão 3.1. Brasília, DF: ICP Brasil, 30 maio 2019. Disponível em: https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-02-v-3-1-polit-seg-da-icp-brasil-pdf. Acesso em: 22 ago. 2020.

KOHN, S. Varejista norte-americana descobre até gravidez de clientes com a ajuda de software. **Olhar Digital**, [*s. l.*], 17 fev. 2012. Disponível em: https://olhardigital.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231. Acesso em: 1° abr. 2020.

LENTO, L. O. B.; FRAGA, J. S.; LUNG, L. C. A nova geração de modelos de controle de acesso em sistemas computacionais. *In*: NAKAHARA, J.; LUNG, L. C. (orgs.). **SBSeg'06** - minicurso no simpósio brasileiro em segurança da informação e de sistemas computacionais. Porto Alegre: SBC, 2006. v. 1, p. 151-201.

LIMA, M. **CP**: Mitnick, um hacker sem computador. **Baguete**, Porto Alegre, 26 jan. 2010. Disponível em: https://www.baguete.com.br/noticias/geral/26/01/2010/cp-mitnick-um-hacker-sem-computador. Acesso em: 1° abr. 2020.

LUZ, É. E. da. **Auditoria e perícia contábil trabalhista**. São Paulo: Pearson, 2016. 128 p.

MACÊDO, D. **Conceito, tipos e características de auditoria de segurança da informação**. Diego Macêdo: um pouco de tudo sobre T.I. [*s. l.*], 29 mar. 2012. Disponível em: https://www.diegomacedo.com.br/conceito-tipos-e-caracteristicas-de-auditoria-de-seguranca-da-informacao/. Acesso em: 1° jul. 2020.

MACHADO, M. J. **Controle de acessos**. **Segurança da Informação**, Curitiba, 2 abr. 2017. Disponível em: https://marceljm.com/seguranca-da-informacao/controle-de-acessos/. Acesso em: 1° abr. 2020.

MAGALHÃES, I. L.; PINHEIRO, W. B. **Gerenciamento de serviços de TI na prática**: uma abordagem com base na ITIL. Porto Alegre: Novatec Editora, 2007. 667 p.

MELO, M. M. de; SANTOS, I. R. dos. **Auditoria Contábil**: atualizada pelas normas internacionais de auditoria. Rio de Janeiro: Freitas Bastos, 2017. 390 p.

MÓDULO. **Gestão de Políticas de Segurança da Informação para TI**. **Módulo**, Rio de Janeiro, c2020. Disponível em: https://www.modulo.com.br/gestao-de-politicas-de-seguranca-da-informacao-para-ti/. Acesso em: 1° abr. 2020.

NAKAMURA, E. T. **Segurança da informação e de redes**. Londrina: Educacional, 2016. 224 p.

PALMA, F. Sistema de gestão de segurança da informação (SGSI). **Portal GSTI**, [*s. l.*], 13 dez. 2016. Disponível em: https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html. Acesso em: 1° abr. 2020.

PANDINI, W. ISO 27000, primeiros passos com a norma. **Ostec Segurança Digital de Resultados**, c2020. Disponível em: https://ostec.blog/padronizacao-seguranca/primeiros-passos-iso-27000. Acesso em: 1° abr. 2020.

PAZ, N. As normas ISO de cibersegurança que sua empresa deve seguir. **Idblog**, [*s. l.*], 31 jul. 2019. Disponível em: https://blog.idwall.co/normas-iso-ciberseguranca/. Acesso em: 1° abr. 2020.

TÜV RHEINLAND, T. Segurança da informação ISO 27001. **TÜV Rheinland Precisely Right**, TI e dispositivos de telecomunicação, São Paulo, c2020. Disponível em: https://www.tuv.com/brasil/br/seguran%C3%A7a-da-informa%C3%A7%C3%A3o-iso-27001.html. Acesso em: 1° abr. 2020.

RODRIGUES, L. **Carregadores públicos podem roubar seus dados; entenda**. **Techtudo**, [s. l.], 3 jun. 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/06/carregadores-publicos-podem-roubar-seus-dados-entenda.ghtml. Acesso em: 1° abr. 2020.

SCHROEDER, T. COBIT and ITIL: differences and similarities. **Excellence Blog**, [*s. l.*], 8 mar. 2016. Disponível em: https://blog.softexpert.com/en/cobit-itil-differences-similarities/. Acesso em: 1° jul. 2020.

SÊMOLA, M. **Gestão da segurança da informação**: uma visão executiva. 2 ed. Rio de Janeiro: Elsevier, 2013. 192p.

SERPRO. Quais são os seus direitos? **Serpro**, Brasília, c2020. Disponível em: https://www.serpro.gov.br/lgpd/cidadao/quais-sao-os-seus-direitos-lgpd. Acesso em: 1° abr. 2020.

SILVA, C. Descubra por que usar uma VPN e veja como escolher a melhor. **Canaltech**, [*s. l.*], c2020. Disponível em: https://canaltech.com.br/internet/descubra-por-que-usar-uma-vpn-e-veja-como-escolher-a-melhor/. Acesso em: 20 fev. 2020.

SOARES, P. V. de C. **Guia LGPD**: lei geral de proteção de dados simplificada. São Paulo: LGPD, 2020. Disponível em: https://conteudo.lbca.com.br/lgpd-guia-simplificado. Acesso em: 1° abr. 2020.

TATICCA. Escopo da auditoria de sistemas. **Allinial Global**, c2020. Disponível em: https://www.taticca.com.br/pt-br/blog/escopo-da-auditoria-de-sistemas. Acesso em: 1° jul. 2020.

TCU. **Boas práticas em segurança da informação**. 4. ed. Brasília: Secretaria de Fiscalização de Tecnologia da Informação, 2012. 103 p.

POSITIVO TECNOLOGIA. Segurança da informação: conheça as 12 melhores práticas. conheça as 12 melhores práticas. **Panorama Positivo**, Curitiba, 15 nov. 2017. Disponível em: https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao/. Acesso em: 1° abr. 2020.

TEIXEIRA, J. P. F. Você: titular de dados pessoais. **Jusbrasil**, [*s. l.*], 24 set. 2019. Disponível em: https://joaopedrofteixeira.jusbrasil.com.br/artigos/760627772/voce-titular-de-dados-pessoais. Acesso em: 1° jul. 2020.

TEIXEIRA FILHO, S. A. **Segurança da informação descomplicada**. Joinville: Clube de Autores, 2019. 516 p.

SILVEIRA, J. C. **Pode ou não pode**: o empregador monitorar e-mail corporativo de trabalhadores. 2017. Brasília: Justiça do Trabalho, Rádio Justiça, 2017. Disponível em: http://www.tst.jus.br/radio-destaques/-/asset_publisher/2bsB/content/pode-ou-nao-pode-o-empregador-monitorar-e-mail-corporativo-de-trabalhadores. Acesso em: 1° abr. 2020.