Tópico 07

Fundamentos de Sistemas de Informação

Segurança da Informação

1. Introdução

Como sabemos, em uma organização, há um conjunto grande de processos e atividades sendo desempenhadas, sendo que os dados e as informações de alguns processos podem alimentar outros processos. Laudon (2011, p.40) afirma que uma empresa pode ser vista como uma coleção de processos de negócios. Isso é importante, pois estamos falando de processos que geram valor à empresa. E mais: Laudon (2011, p.40) afirma que as informações são o meio de comunicação com os parceiros de negócio da empresa. Sendo assim, estamos falando de um ambiente perigoso, aberto a princípio, em que há um fluxo de informações transitando "valor" entre dois entes, o que requer que um grau maior de proteção seja providenciado àquele fluxo.

Esta unidade tem como principal objetivo descrever esse ambiente organizacional onde o principal ativo da organização irá trafegar: a informação. É muito importante que os ativos informacionais sejam mapeados, mensurados seu valor, identificados "gargalos", suas ameaças, fragilidades e potenciais ataques à sua integridade. Estamos procurando defender a informação em alguns de seus principais atributos que são a consistência, integridade e disponibilidade.

Nesse sentido, toda e qualquer organização estará sujeita à ação de criminosos e comportamentos antiéticos das pessoas, o que pode vir a gerar grande impacto financeiro aos negócios. De acordo com Prado (2014, p.59), algumas dessas ameaças podem ser identificadas como **fraudes**, referindo-se a qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar

outrem, ou de não cumprir determinado dever. Por exemplo: podemos encontrar fraudes financeiras e comerciais, como sugestões via internet para investir em ações em crescimento de empresas, ou mesmo fraudes tecnológicas, como sites falsos de bancos, sorteio vencedor na loteria federal e e-mails com vírus. Conforme descrito pelo autor, uma **fraude** aproveita a ingenuidade e a vulnerabilidade das pessoas que, muitas vezes, estão em situações difíceis ou frágeis, para extorqui-las ou enganá-las. Outros tipos de ameaças referem-se aos **crimes eletrônicos (ou cibernéticos), ameaças virtuais, engenharia social, terrorismo digital, ciberespionagem,** dentre outros, sendo que os principais serão mais bem discutidos nas próximas seções. Exame (2020) aponta que:

> *"O Brasil sofreu **15 bilhões de tentativas de ataque cibernético em apenas três meses**, de acordo com levantamento divulgado nesta terça-feira pela empresa de segurança cibernética Fortinet. O dado foi obtido a partir de clientes da companhia no país e de dados fornecidos por entidades de classe. O estudo detectou que o Brasil segue sendo um alvo mundial importante para criminosos cibernéticos e que ainda está bastante vulnerável a ataques antigos como os usados no Wannacry, em 2017, e os que violaram bancos no Chile e no México em 2018. Segundo a empresa, a eficácia desse tipo de ataque indica que ainda existem sistemas não corrigidos ou atualizados em empresas no país. Como é a primeira edição do levantamento, não há um comparativo em relação a períodos anteriores" (grifo meu).*

Nesse mesmo sentido de apontar a gravidade da situação de segurança das informações, o Senado (2020) diz que o Brasil é 2º no mundo em perdas por ataques cibernéticos, sendo que, em 12 meses, entre 2017 e 2018, os prejuízos advindos dos ataques cibernéticos no Brasil ultrapassaram **US$ 20 bilhões**

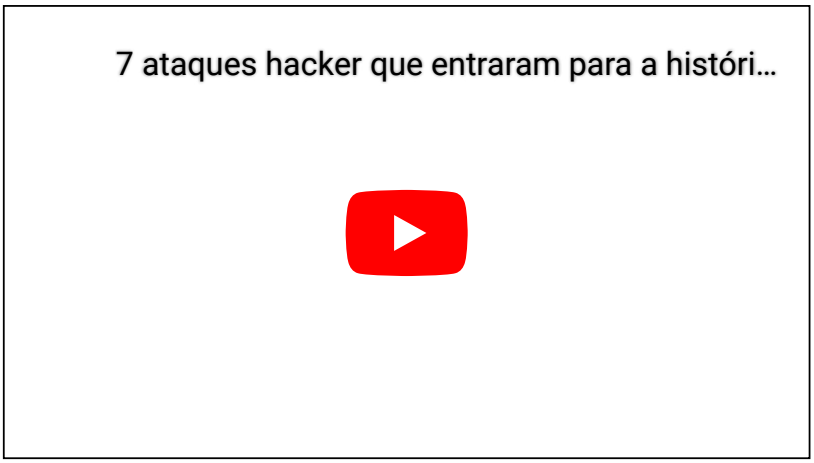
(mais de R$ 80 bilhões). É claro que esse volume de ameaças (e prejuízos) não passaria despercebido pelas organizações. De acordo com AON (2020), “Risco Cibernético” é atualmente uma das 10 principais preocupações dos executivos, já sendo um risco levado muito a sério em países como Estados Unidos e Europa, e que vem ganhando muita relevância no Brasil nos últimos anos, pois diz respeito a ataques que afetam tanto pessoa física como jurídica.

À medida que as companhias avançam em suas plataformas digitais, com a implementação de sofisticados sistemas de tecnologia, cresce o temor de possíveis ataques cibernéticos – sabotagem, roubo ou até sequestro de dados e informações vitais. Essa preocupação faz sentido. Segundo a empresa global de segurança de informação SonicWall, o ano de 2018 já bateu recorde nesse tipo ameaça. Em seu relatório semestral, a empresa estima que foram registrados 6 bilhões de ameaças a sistemas de rede pelo mundo de janeiro a junho. O número é mais que o dobro do apontado no mesmo período de 2017. O tema é tão relevante que foi um dos principais temas do Fórum Econômico Mundial 2018, na Suíça. Alois Zwinggi, diretor geral do fórum e líder do Centro Global de Segurança Cibernética, chegou a dizer em Davos que “se queremos evitar uma era de escuridão digital, precisamos trabalhar mais para garantir que os benefícios e o potencial da Quarta Revolução Industrial sejam seguros para a sociedade”. Portanto, segurança cibernética (ou cybersecurity, no termo em inglês) é a palavra de ordem.

Fonte: MELLO (2020)

uanto aos aspectos legais envolvidos com a segurança da informação, há um amplo conjunto de normas e leis (no sentido amplo) estabelecidas no Brasil que buscam proteger os cidadãos e as empresas em seus ativos. A **Constituição Federal Brasileira,** de 1988, assegura a inviolabilidade do direito à privacidade, seguindo a orientação internacional, em seu artigo 5º, inciso X, ao estabelecer que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". No Brasil, o direito à privacidade tem como objetivo resguardar aspectos pessoais, familiares **e empresariais.** Mais recentemente, o Marco Civil da Internet (Lei 12.965/2014), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil bem como a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018) inovaram na defesa dos preceitos estabelecidos na Constituição Federal, tentando proteger, de forma efetiva, os direitos do consumidor e do indivíduo quanto a seus interesses comerciais e de dignidade da pessoa humana. São todos esses arcabouços legais e normativos que um profissional de Tecnologia da Informação deve se basear para realizar suas atividades profissionais e comerciais.

O vídeo apresenta um histórico dos principais ataques cibernéticos mais recentes no mundo, que geraram milhões de dólares de prejuízos às suas organizações e clientes. É ressaltada a importância de investimentos em dispositivos de segurança pelo cidadão e pelas empresas. Vale como exemplo para qualquer profissional de TI.



2. Conceitos de Segurança de Dados e Formas de Proteção

Antes de discutirmos o conceito de segurança da informação, precisamos mensurar o grau de sensibilidade desse importante ativo na organização, isto é, precisamos fornecer um grau de importância aos diferentes tipos de informações existentes nas empresas para, posteriormente, determinarmos suas prioridades de ações de defesa. De acordo com Lyra (2015, p. 12), há uma escala de **cinco níveis de sensibilidade** a ser atribuída a cada conjunto de informações referentes a uma mesma entidade ou conceito, que são:

1. **Nível 1 – Informação pública** – Informação que foi obtida sem ônus, de fontes públicas, ou que foi produzida internamente pela empresa, mas que tem interesse público. Essas informações não precisam de controle de acesso e de distribuição.
2. **Nível 2 – Informação restrita –** Informação que foi adquirida de terceiros com cláusula de sigilo, mas que outras empresas também podem adquirir, ou que foi produzida pela empresa e que tem interesse restrito a ela. Essas informações, se vazadas, podem comprometer a imagem da organização, mas não sua operação.
3. **Nível 3 – Informação sigilosa** – Informação que foi obtida, com exclusividade, de terceiros, ou que foi produzida pela empresa e que trata de decisões, processos ou produtos críticos para a sua operação. Essas informações, se vazadas ou danificadas, podem gerar decisões erradas e prejudiciais para a operação da empresa

ou inviabilizar o lançamento de um novo produto ou serviço. São exemplos de informações de nível 3 relatórios de investigação de práticas concorrenciais ilegais, detalhes sobre campanhas de lançamento comercial, detalhes sobre planos de fusão, aquisição ou fechamento de empresas;

4. **Nível 4 – informação secreta** –Informação referente a detalhes de produtos e serviços que estão em processo de desenvolvimento ou decisões sobre significativas alterações do valor patrimonial da empresa. Essas informações, se vazadas ou danificadas, podem comprometer o protagonismo no lançamento de um novo produto ou ainda permitir que concorrentes o lancem antes da empresa. São exemplos de informações detalhes de produtos e serviços em desenvolvimento, detalhes sore a negociação de compra ou venda de empresas ou filiais, relatórios sobre falhas graves, em produtos, serviços ou processos internos, que podem afetar o valor das ações da empresa na bolsa de valores;
5. **Nível 5 – Informações ultrassecretas** – Informações sobre atos e fatos da organização cujo acesso é limitado apenas a mais alta direção executiva e seus acionistas. Essas informações, se vazadas, podem levar a ações judiciais à empresa ou a seus executivos e acionistas. Compreendem ainda informações sobre segredos industriais que diferenciam a empresa de seus concorrentes.

Em Lyra (2015, p. 20), a **Segurança da Informação** é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade (CID), não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou em papel.

De acordo com TCU (2012, p.9), a **Segurança da Informação (ou de dados)** visa garantir a **integridade, confidencialidade, autenticidade e disponibilidade** das informações processadas pela instituição, levando-se em consideração seu nível de sensibilidade como descrito anteriormente. Conforme explica o autor:

> *"A integridade consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação a inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A* ***manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital****" (grifo nosso).*
>
> *(TCU, 2012, p.9)*

Já a autenticidade, segundo ainda TCU (2012, p.9), refere-se à garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações. A disponibilidade consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a **prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.** A confidencialidade é a propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não-autorizados.

Além dessas características básicas associadas à segurança das informações, temos ainda a **criticidade**, que é a classificação da informação de acordo com o grau de relevância do ativo de informação em relação à confidencialidade, integridade e disponibilidade, observadas as necessidades do negócio e a legislação em vigor, o **não-repúdio ou irretratabilidade** como sendo a garantia de que uma pessoa não consiga negar a autoria ou envio de uma informação e, por fim, a **proporcionalidade**, em que a organização, em seu poder discricionário (decisão), buscará subsídios na forma da lei,

em conceitos, normas e princípios que deverão ser observados em cada caso concreto, dentro do critério de razoabilidade (TJMS, 2020).

Os 5 pilares da Segurança da Informação.

Outro conceito muito importante para a segurança da informação é o que chamamos de "**Ativos de Informação**". Conforme disposto em Lyra (2015, p. 21):

> *"Um ativo de informação é 'qualquer coisa que tenha valor para organização'. Portanto,* ***podem existir diversos tipos de ativos incluindo a própria informação*** *(contratos e acordos, documentações de sistema, bases de dados, manuais de usuário, trilhas de auditoria, planos de continuidade, etc.), pessoas e suas qualificações/experiências, ativos de software (sistemas, aplicativos, ferramentas, etc.), ativos físicos (mídias Governança da Segurança da Informação removíveis, equipamentos computacionais, equipamentos de comunicação, etc.), serviços (iluminação, eletricidade, refrigeração, etc.) e aqueles que são intangíveis, como é o caso da reputação da organização" (grifo nosso).(LYRA, 2015, p. 21)*

De acordo com esse autor, um dos fatores críticos de sucesso para a garantia da segurança da informação é a **correta identificação, controle e constante atualização dos**

diferentes tipos de ativos (inventário). Com a finalidade de alcançar uma correta proteção, torna-se importante conhecer o que seria a Gestão de Ativos. Como princípio básico, é recomendado que todo ativo seja identificado e documentado pela organização. A cada um deles deve-se estabelecer um proprietário responsável que lidará com a manutenção dos controles. Controles estes que podem ser delegados a outros profissionais, porém, sempre sob a responsabilidade do proprietário. A figura a seguir apresenta os principais ativos de informação a serem gerenciados na empresa.

Principais Ativos no escopo da Segurança da Informação.

Algumas ações maliciosas podem atuar sobre usuários dos sistemas, tendo sido conhecidas como ataques de “Engenharia Social”. Estas ações serão descritas a seguir, mas, basicamente, referem-se a identificar comportamentos frágeis nas pessoas que as fazem, sem intenção, entregar ou disponibilizar a informação. É o caso, por exemplo, de quando um funcionário na empresa recebe uma ligação de alguém se dizendo do setor de TI e que está solicitando sua senha de acesso à rede para eventuais testes.

Um ativo intangível é aquele que não possui um valor monetário determinado, fixado, como, por exemplo, a imagem da empresa junto ao mercado. Imagine a situação de uma empresa que possui milhões de clientes cadastrados sofrer um ataque e ter os dados de seus clientes acessados de forma indevida. Definidos os “Ativos de Informação”, precisamos determinar suas fragilidades, ou **vulnerabilidades**, que, segundo Coutinho

(2017), podem ser exploradas por uma ou diversas ameaças que podem ocasionar danos.

2.1 AMEAÇAS E SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO

Independente de como seja a organização, é necessário se pensar numa metodologia para implantar rotinas de segurança da informação. Uma área muito forte para os profissionais de Tecnologia da Informação envolve a Gestão da Segurança da Informação – GSI. Essa gestão envolve, dentre outras ações, um planejamento, a implementação, seu gerenciamento (controle) e, por fim, suas correções e evoluções. Dentro das ações necessárias da GSI, está a identificação de **Ameaças e Riscos** aos ativos de informação. De acordo com Oliveira (2020), as Ameaças que, normalmente, não podem ser controladas, são um evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso (ativo). As ameaças normalmente aproveitam das falhas de segurança da organização. A ameaça é a possibilidade de um agente (ou fonte de ameaça) **explorar acidentalmente ou propositalmente uma vulnerabilidade específica.** Já os Riscos, de acordo com o autor, são externos e/ou internos, e podem ser minimizados ou mitigados. Um Risco é qualquer evento que possa causar impacto na capacidade de empresas atingirem seus objetivos de negócio. É uma **probabilidade** de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto (em geral, negativo) para a organização.

Já em HSC (2020), as principais ameaças são identificadas e catalogadas para o ano 2020, sendo elas:

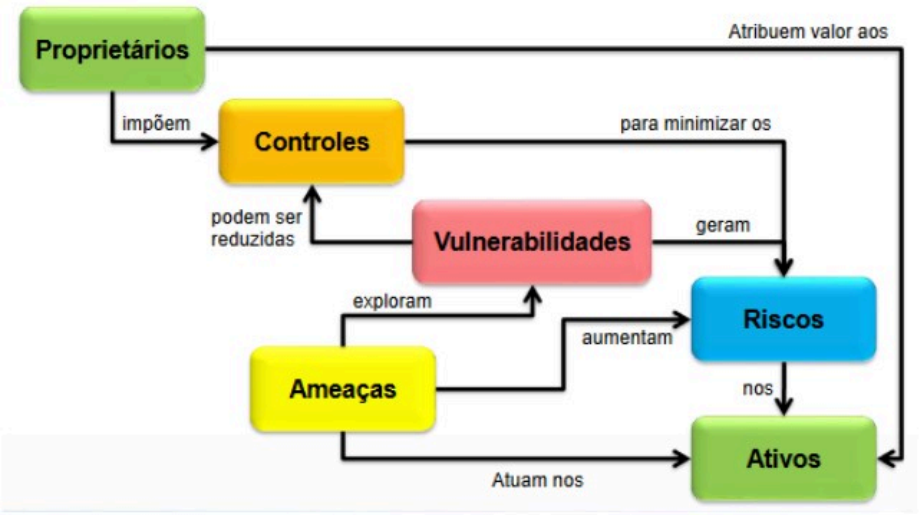
1. **Ataques direcionados:** diferentemente dos ataques em massa e automatizados, os ataques direcionados utilizam informações específicas de uma organização para executar um ataque. O criminoso, neste caso, estuda a empresa e faz uso de técnicas de

engenharia social para induzir os profissionais ao erro, como fazer um depósito em uma conta ou pagar um boleto.

2. **Ataques persistentes avançados:** também conhecidos como APT (Advanced Persistent Threats), são utilizados para descrever um tipo de ataque direcionado, focado em espionagem via internet. As ameaças persistentes avançadas são descritas desta forma, pois, na maioria das vezes, são invasores contratados para atacar uma empresa específica. Essas tentativas de invasão só irão cessar após o objetivo final ser atingido, o que pode, às vezes, demorar meses.
3. **Ataques a dispositivos IoT:** a Internet das Coisas (IoT) oferece uma série de benefícios para as empresas, mas também traz a necessidade de investir em segurança. Os ataques aos dispositivos com IoT podem copiar ou comprometer os dados transmitidos por eles, possibilitando a espionagem industrial ou mesmo a danificação do sistema como um todo.
4. **Adwares**: constituem um tipo de malware criado para apresentar anúncios não solicitados na tela dos usuários via navegador web, podendo abrir nova abas, alterar a página inicial ou redirecionar para sites não seguros ou impróprios.
5. **Business E-mail Compromise:** também conhecido como fraude do CEO, o business e-mail compromise é um ataque em que o criminoso envia uma mensagem se passando por um profissional de alto cargo, como o presidente da empresa. No conteúdo do e-mail, enviado em caráter de urgência, pode ser solicitada uma transferência imediata para determinada conta bancária. Também pode ser utilizado um boleto para a concretização do ataque.
6. **Documentos maliciosos:** constituem um tipo de malware que explora vulnerabilidades de documentos do padrão Office, como arquivos .doc, .docx, .ppt, .pptx, .xls, .pdf, entre outras extensões.
7. **Engenharia social:** um ataque via engenharia social engana a vítima sem utilização de uma única linha de código ou conhecimento sobre segurança da informação. Os criminosos exploram a psicologia humana, a única fraqueza encontrada em toda e qualquer empresa. Geralmente, o criminoso se passa por alguém confiável e a própria vítima passa seus dados pessoais de livre e espontânea vontade.
8. **Malwares**: constituem um software malicioso que têm como objetivo danificar dados ou agir no sistema da vítima sem sua autorização. Ele pode, por exemplo, deletar arquivos ou fazer com que o IP do usuário acesse um determinado site sem que ele saiba — isso é feito em larga escala para derrubar sites de organizações para prejudicá-las.

9. **Phishing**: é uma prática que visa roubar dados cadastrais de clientes por meio de mensagens iscas, geralmente, por e-mail. Ao clicar em um link que supostamente levaria à compra de um produto, são solicitados os dados do usuário que, posteriormente, são utilizados para outras fraudes.
10. **Spyware**: ataca computadores ou dispositivos móveis para coletar informações sobre seus usuários. É considerada uma ameaça sorrateira; geralmente, atua abrindo caminho no sistema operacional sem o consentimento da vítima.
11. **Trojan**: também conhecido como Cavalo de Troia, o trojan é um software que se passa por um programa legítimo, simulando alguma funcionalidade útil. Esta ameaça abre uma porta para que um hacker tenha acesso ao seu computador para roubar senhas ou qualquer outro tipo de dado sigiloso que possa ser usado para extorquir a vítima.

A figura a seguir ilustra como os elementos contextualizados na GSI estão numa relação de causa-efeito. É importante, nesse ponto, relatar a necessidade de imposição de políticas e rotinas de Controle sobre os riscos nos ativos, devendo, a todo custo, ser minimizados.



Relação de causa/efeito entre os elementos da Segurança da Informação.

Dentro desse volume grande de procedimentos e conceitos de Segurança da Informação, há algumas soluções do ponto de vista de recomendações ou padrões normativos disponíveis para empresas de qualquer porte e segmento. Alguns desses conteúdos são de reconhecimento internacional, como um

conjunto de normas e práticas a serem planejadas, implementadas, controladas e ajustas, de forma a garantir ao máximo um bom nível de segurança da informação na empresa.

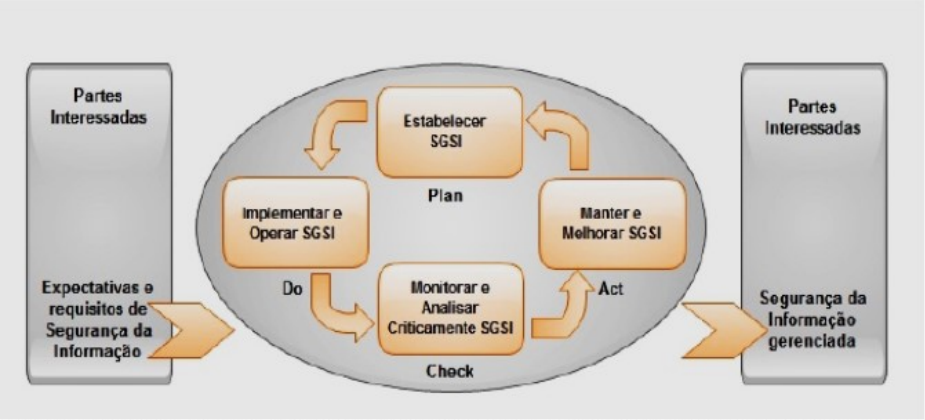
O texto aqui referenciado descreve os principais conceitos, processos e ferramentas associados à Segurança da Informação. É um material bem amplo e descreve também uma visão prática da implementação de software focado em segurança de dados, além de apresentar um conceito de auditoria em sistemas de informação quanto à sua segurança. É uma fonte de leitura completa.

http://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_IFRO-Seguranca_Informacao_04_04_14.pdf?sequence=1&isAllowed=y

Dentre esses conteúdos, podemos citar as normas ISO – International Organization for Standardization. A norma **ISO 27001** é uma norma que define os requisitos para um **Sistema de Gestão da Segurança da Informação (SGSI).** Conforme descrito por Palma (2020, s/n):

> *"O SGSI é descrito como um sistema parte do sistema de gestão global da organização, com base em uma abordagem de risco do negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. O SGSI inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos" (grifo nosso).*

Conforme detalha o autor, a ISO 27001 é a principal norma que uma organização deve utilizar como base para obter a certificação empresarial em gestão da segurança da informação. Por isso, **é conhecida como a única norma internacional auditável que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI).** A figura a seguir apresenta uma visão geral dos principais processos associados à norma.



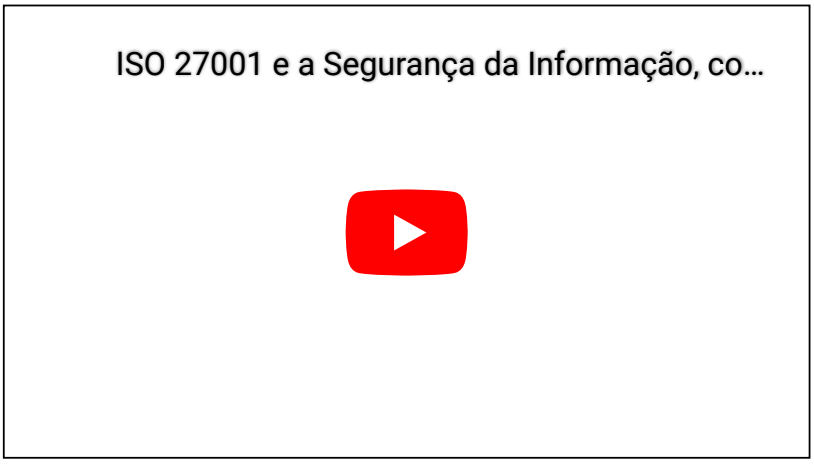
Processos principais da norma ISO 27001.

> *"A norma ABNT NBR ISO/IEC 27001 tem por objetivo '**prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação**' (ABNT NBR ISO/IEC 27001, 2013, item 0.1). Para cumprir com seu objetivo, a ABNT NBR ISO/IEC 27001 utiliza o **modelo PDCA (Plan-Do-Check-Act),** esse modelo tende a garantir melhoria contínua do Sistema de Gestão de Segurança da Informação, para melhor entendimento desse modelo" .*
>
> *(grifo nosso)*

Ainda de acordo com Palma (2020), a outra norma ISO de grande relevância para a Gestão da Segurança da informação é a norma ISO 27002, é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação. Segundo o autor, **é**

recomendável que a norma seja utilizada em conjunto com a ISO 27001, mas pode ser também consultada de forma independente com fins de adoção das boas práticas. Para Oliveira (2017, p. 7), a ISO 27002 tem por objetivo sugerir boas práticas de gestão de segurança da informação para as organizações, através da seleção, implementação e gerenciamento de controles baseados nos ambientes organizacionais. A **norma também permite que a organização crie seus próprios controles adequando-se as suas necessidades, ou utilize controles de outro conjunto.**

O vídeo apresenta, em uma entrevista, alguns conceitos sobre normas ISO de segurança da informação, em especial, as normas 27001 e 27002. O vídeo aborda, de forma didática, como as normas devem ser implementadas e quais os resultados esperados com sua adoção.



3. A Lei Geral de Proteção de Dados Pessoais (LGPD) e o

Conceito de Desenvolvimento Orientado à Proteção de Dados

A Lei 13.709/2018, conhecida como a Lei Geral de Proteção de Dados Pessoais – LGPD, 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. Essa norma dever ser amplamente observada por qualquer profissional de Tecnologia da Informação no manuseio de dados pessoais. Dentre outros aspectos, a lei foca no cuidado da Identificação dos dados (pessoal, sensível, criança, público, anonimizado), departamentos, meios (físico ou digital), operadores internos e externos para mensuração de exposição da empresa à LGPD. Em caso de algum incidente sobre os dados mantidos, o responsável pelo tratamento desses dados deve comunicação aos órgãos fiscalizatórios (ANPD, Procon, Senacon) e à imprensa sobre incidente de segurança que acarrete risco ou dano. E, principalmente, **deve adotar medidas de segurança da informação aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.** As multas pelo não cumprimento de seus preceitos podem variar de 2% do faturamento da empresa até 50 milhões de reais.

A LGPD estabelece o **Data Protection Officer – DPO (Encarregado),** que é a pessoa física ou jurídica cuja responsabilidade é atribuída à empresa para exercer as atividades previstas na LGPD. Dentre outras atribuições, o DPO deve orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. Assim, este profissional deverá orientar as equipes de desenvolvimento de software sobre como desenvolver produtos com foco na gestão de dados. O propósito é inserir nos programas e arquiteturas de software todos os mecanismos

possíveis para a proteção de dados de seus clientes, sob pena de responsabilização. Essa é uma mudança de paradigma muito forte e que todo profissional de TI deverá conhecer para atendimento às normas legais e evitar prejuízos futuros sob o ponto de vista criminal.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709/2018, tem como objetivo regulamentar o tratamento de dados pessoais pelas empresas, uma vez que os dados pessoais ganharam grande importância na economia moderna, pois permitem fazer predições, analisar perfis de consumo, opinião, entre outras atividades. Hoje, mais de 126 países no mundo possuem leis para a proteção de dados pessoais visando à regulamentação do tratamento de dados das empresas, evitando-se o mau uso destes, bem como a responsabilização das empresas por isso e por incidentes e acidentes com dados pessoais. Nessa lei, o tratamento de dados é visto como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Fonte: CAMARGO (2020).

4. Conclusão

Esta unidade abordou um tema de alta relevância a todo profissional de Tecnologia da Informação, que é a segurança da informação. Percebemos a importância da adoção de práticas de gestão da segurança da informação, conhecendo seus principais conceitos e sabendo que os ativos de informação devem ser protegidos. De imediato, vimos como mensurar a importância de uma informação através de sua sensibilidade. Por fim, vimos que há algumas normas e padrões de reconhecimento mundial que nos permitem adotar essas práticas de proteção de forma sistematizada, especialmente, as normas ISO 27001 e 27002. No Brasil, entendemos como as normas e leis estão sendo criadas e implementadas com foco em segurança de dados pessoais quando discutimos a LGPD.

5. Referências

AON. **Relatório de Riscos de Segurança Cibernética 2019**. Disponível em https://www.aon.com/brasil/consulting/riscos-ciberneticos.jsp, acessado em 10/06/2020.

CAMBIUCCI, W. **Uma introdução sobre Cybersecurity e LGPD**. Disponível em https://cloudblogs.microsoft.com/industry-blog/pt-br/cross-industry/2019/10/29/introducao-sobre-cybersecurity-lgpd/, acessado em 10/06/2020.

CAMARGO, L.B. Guia LGPD – **Lei Geral de Proteção de Dados Simplificada.** Disponível em https://d335luupugsy2.cloudfront.net/cms/files/92859/1565723282Guia_-_LGPD.pdf, acessada em 16/06/2020.

COUTINHO, M..M, SANTOS, R.N., CUSTODIO, V.H.S., AMARAL, E. C., SABINO, E., ABE, N. **Estudo de Caso: Principais Pilares da Segurança da Informação nas**

Organizações. Revista Gestão em Foco, Ed. nº 9. 2017. disponível em http://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/052_estudo5.pdf, acessado em 10/06/2020.

EXAME. **A evolução das Plataformas de T Brasil sofreu 15 bilhões de ataques cibernéticos em 3 meses, diz estudo**. Disponível em https://exame.com/tecnologia/brasil-sofreu-15-bilhoes-de-ataques-ciberneticos-em-3-meses-diz-estudo/, acessado em 14/06/2020.

FONSECA, P.F. **Gestão de Segurança da Informação: O Fator Humano.** Disponível em https://www.academia.edu/33539394/Gest%C3%A3o_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_O_Fator_Humano, acessado em 10/06/2020.

HSC. **Conheça as principais ameaças virtuais em 2020.** Disponível em https://www.hscbrasil.com.br/principais-ameacas-virtuais/, acessado em 12/06/2020.

LAUDON, K.C., L., J.P.. **Sistemas de Informação Gerenciais.** 9 ed. São Paulo – SP: Editora Pearson, 2011.

LYRA, M.R. **Governança de Segurança da Informação.** Edição do Autor – Brasília – DF. 2015. disponível em https://www.academia.edu/38775927/Mauricio_Rocha_Lyra_-_Governan%C3%A7a_em_Sistemas_de_Informa%C3%A7%C3%A3o, acessado em 13/06/2020.

OLIVEIRA, T.R. **Implantação de políticas de segurança da informação em uma pequena empresa**. Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica. Vol. 8, Numero 1. 2017. Disponível em https://www.google.com/url?sa=i&url=http%3A%2F%2Fperiodicos.unifacef.com.br%2Findex.php%2Fresiget%2Farticle%2Fdownload%2F1332%2F1040&psi

g=AOvVaw2hDLvgGYtvymUnXW2ykfmb&ust=1592418226026000&source=images&cd=vfe&ved=0CAMQjB1qFwoTCPD31q_6huoCFQAAAAAdAAAAABAD, acessado em 13/06/2020.

MARTINS, A.B., SANTOS,C.A.S. **Uma Metodologia para Implantação de um Sistema de Gestão De Segurança da Informação.** Revista de Gestão da Tecnologia e Sistemas de Informação, Vol. 2, Numero 2. 2005. disponível em https://www.scielo.br/pdf/jistm/v2n2/02.pdf, acessado em 12/06/2020.

MELLO, K., TEIXEIRA, L.B. **Por que estamos na era da proteção da informação.** Disponível em https://forbes.com.br/negocios/2019/01/por-que-estamos-na-era-da-protecao-da-informacao/, acessada em 12/06/2020.

OLIVEIRA, W. **Riscos, Vulnerabilidade E Ameaça Em Segurança Da Informação.** Disponível em https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/, acessado em 10/06/2020.

PALMA, F. **As normas da família ISO** 27000. Disponivel em https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html, acessado em 13/06/2020.

PRADO, E., ARAÚJO, L., ORNELAS, R.. **Fundamentos de Sistemas de Informação.** Ed. 1. Editora Elsevier. São Paulo – SP, 2014.

SENADO. **Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência.** Disponível em https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia, acessado em 10/06/2020.

SCHROEDER, G.L. **Conceitos Gerais – Segurança da Informação**. Disponível em

https://gustavoschroeder.wordpress.com/2017/11/20/conceitos-gerais-seguranca-da-informacao/, acessado em 12/06/2020.

TCU. **Boas Práticas em Segurança da Informação.** Disponível em http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf, acessado em 05/06/2020.

TJMS. **RESOLUÇÃO N. 109, DE 13 DE AGOSTO DE 2014.** Disponível em https://www.tjms.jus.br/legislacao/visualizar.php?lei=29518&original=1, acessado em 05/06/2020.

FERNANDES, N.O.C. **Segurança da Informação.** Universidade Federal do Mato Grosso – UFMT. Cuiabá – MT. 2013. Disponível em http://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_IFRO-Seguranca_Informacao_04_04_14.pdf?sequence=1&isAllowed=y, acessado em 12/05/2020.

YouTube. (2018). 7 ataques hacker que entraram para a história. 8min03. Disponível em:< https://www.youtube.com/watch?v=IvgR6tlusr0 >.

YouTube. (2020). **ISO 27001 e a Segurança da Informação, com Bushidô Academy.** 17min38. Disponível em:< https://www.youtube.com/watch?v=0QMAM3Wr8IQ>.

Parabéns, esta aula foi concluída!

O que achou do conteúdo estudado?

Péssimo Ruim Normal Bom Excelente

Deixe aqui seu comentário

Mínimo de caracteres: 0/150

Enviar