SEGURANÇA NA TRANSMISSÃO DE DADOS:
O Papel da Informação e a Segurança no Mundo Digital

Gabrielle Teixeira Monteiro[1]
Laura Romero dos Santos[2]

RESUMO

No presente artigo, procurou-se desenvolver um estudo da norma NBR ISO/IEC 27002. Para isso descrevemos os principais aspectos referentes à Segurança da Informação, definimos alguns conceitos, princípios e demonstramos algumas ameaças e alguns elementos de Segurança de Dados. Além disso, procurou-se demonstrar a Política de Segurança e a sua importância para uma empresa. Assim como a importância da política de segurança nos dias atuais, as etapas para construção de uma política confiável e que não fuja da cultura da empresa, e para tanto, nos baseamos na norma NBR ISO/IEC 27002.

Palavras-Chave: Informação. Segurança. Criptografia. Digital. Empresa.

[1] Acadêmica do Curso Superior em Tecnologia em Sistemas para Internet – Faculdade Alcides Maya - gabriellemonteiro0902@gmail.com

[2] Estudante do Curso Técnico em Informática na Instituição Alcides Maya - lauraduka17@gmail.com

INTRODUÇÃO

O presente artigo tem por objetivo apresentar de uma forma clara e sucinta a respeito dos principais conceitos, finalidades e princípios da segurança da informação, mostrando que está diretamente ligada com a proteção de um conjunto de dados, de forma a preservar o valor que possuem para um indivíduo ou uma organização.

Segundo fontes extraídas da Fundação Bradesco (2017), antigamente a informação era algo a ser guardado em pastas ou gavetas, em salas que na maioria das vezes o acesso era restrito, porém nos dias de hoje muitas das informações ficam armazenadas na *internet,* que possui inúmeros recursos de armazenamento de dados, nem todos são seguros, mas mesmo assim milhares de usuários fazem seu uso para guardar desde informações simples e cotidianas até mesmo documentos sigilosos, fotos pessoais, etc.

Exercendo papel cada vez mais relevante no cotidiano, a tecnologia da informação vem se expandindo cada vez mais, por isso, torna-se indispensável discutir a importância de proteger essas informações e também quanto aos riscos e às ameaças que se apresentam nesta área. Como já citado a segurança da informação é um assunto importante para todos, pois afeta diretamente todos os negócios de uma empresa ou de um indivíduo, a mesma é um elemento essencial para a geração do conhecimento, para a tomada de decisões, e que representa efetivamente valor para o negócio.

Faz-se então importante saber o uso da segurança na transmissão e armazenamento de dados, saber os principais conceitos e como se proteger de *crackers, ataques cibernéticos e, entre outros.*

> Nota-se que normalmente as pessoas são o elo mais frágil quando o assunto é segurança da informação, as soluções técnicas não contemplam totalmente sua segurança, desta forma torna-se necessário que os conceitos pertinentes a segurança sejam compreendidos e seguidos por todos dentro da organização, inclusive sem distinção de níveis hierárquicos. (MOREIRA, 2008).

Princípios da Segurança da Informação

Segundo Oliveira (2017), a partir do momento em que as informações são expostas sem um consentimento prévio, isso pode ser caracterizado como uma invasão. Para a proteção de informações valiosas, é preciso aplicar os princípios básicos da segurança da informação.

A segurança da informação segue por 4 princípios básicos:

- Autenticidade;
- Confidencialidade;
- Disponibilidade; ● Integridade.

Autenticidade na segurança da informação serve para “provar” que o usuário é realmente quem ele diz ser, um exemplo claro disso é quando vamos fazer login em redes sociais, temos que entrar com nosso *e-mail* e *senha*. Dessa forma, a autenticidade atua gerando uma documentação sobre qualquer manipulação de dados no sistema.

Confidencialidade é quando algo, algum documento é confidencial, poucos usuários podem ter acesso, geralmente são arquivos ou documentos protegidos por senhas ou até mesmo criptografados. Como exemplo, podemos citar os bancos e outras instituições financeiras que, por lei, são obrigadas a proteger os dados pessoais dos clientes. Se houver algum tipo de vazamento, são responsabilizados pelos danos causados.

Disponibilidade, termo usado para quando arquivos, dados ou documentos importantes necessitam estar disponível para os usuários a qualquer momento. Por exemplo, empresas como a Amazon dependem que seus servidores estejam no ar 24 horas por dia, 7 dias por semana e nos 365 dias do ano, pois o negócio funciona inteiramente na web. Já um profissional de vendas pode se contentar em esperar por

um relatório de desempenho no dia seguinte. Uma solução para a boa disponibilidade pode ser migrar o Data Center para a nuvem.

Integridade é a garantia de que a mensagem sairá de sua origem e chegará igual ao seu destino, sem sofrer alterações. Isso aumenta o nível de confiabilidade do banco de dados e informações da empresa, pois assegura que eles sejam editados somente por pessoas autorizadas, mantendo o estado original quando armazenados. Sistemas de criptografia de dados são amplamente adotados para se conseguir bons níveis de integridade.

Para uma segurança eficaz dos dados, sem dúvidas sua empresa precisa criar uma política de segurança da informação. Onde terá diversos processos e rotinas, que visam a resguardar ao máximo os arquivos da empresa. Iniciando melhorias como: backup, antivírus, IDS, firewall, monitoramento de pacotes, entre outras formas. Outra implementação importante são os testes de penetração, eles visam testar o sistema da empresa detectando vulnerabilidades e falhas. (OLIVEIRA, 2017)

Política de Segurança da Informação

A *Política de Segurança da Informação (PSI)* é um documento que precisa abranger um conjunto de normas, métodos e procedimentos, que devem ser comunicados a todos os funcionários, assim como deve ser revisado periodicamente. O *Sistema de Gestão de Segurança da Informação* (*SGSI)* garante a viabilidade e o uso correto somente por pessoas autorizadas. (FONTES, 2006)

Para elaborar uma PSI, deve-se levar em conta a NBR ISO/IEC 27001:2005, uma norma para a gestão de segurança da informação, que auxilia as melhores práticas para implementar, manter e melhorar a gestão de segurança da informação em uma organização.

Conforme a ISO/IEC 27002:2005(2005), a informação é um conjunto de dados que apresenta um ponto de vista, é isso que gera uma informação. Um dado não tem valor antes de ser processado, a partir do seu processamento, ele passa a ser considerado uma informação, que pode gerar algum conhecimento. Portanto, podese entender que informação é o conhecimento produzido como resultado do processamento de dados.

Segundo a NBR ISO/IEC27002 (2005), é recomendado que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua contínua pertinência, adequação e eficácia.

Classificação da Informação

Conforme pesquisas elaboradas pela Escola Virtual Fundação Bradesco (2017) a segurança na transmissão de dados classifica-se em quatro tópicos sendo eles: pública, confidencial, interna e secreta.

Pública: É a mais comum das informações, a que pode vir a público sem consequências danosas ao funcionamento normal da organização e cuja integridade não é vital.

Interna: O acesso a esse tipo de informação deve ser evitado, embora as consequências do uso desautorizado não sejam por demais sérias. Sua integridade é importante, mas não é vital.

Confidencial: É quando a informação é restrita aos limites da organização, cuja divulgação ou perda pode levar ao desequilíbrio operacional e, eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente.

Secreta: É a informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

Riscos na Segurança da Informação

Alguns dos principais riscos e mais comuns da segurança digital estão entre a vulnerabilidade, agentes mal-intencionados e os riscos (furtos de dados, perdas financeiras, danos à imagem e até mesmo uma perda de confiança na tecnologia).

Além disso, é importante destacar que a análise de risco da informação possui três objetivos principais: identificar riscos, quantificar o impacto das prováveis ameaças e conseguir um equilíbrio financeiro entre o impacto do risco e o custo da contramedida.

Figura 1 - Ameaças na Segurança da Informação

Fonte: Fundação Bradesco

Vulnerabilidade

Vulnerabilidade pode ser considerada como uma falha de procedimento, implementação, ou controles internos de um sistema que pode ser propositalmente explorado, resultando em uma brecha de segurança e violação da política de segurança do sistema.

Já em segurança de computadores, vulnerabilidade é uma fraqueza que permite que o atacante reduza a garantia da informação do sistema. A vulnerabilidade é a interseção de três elementos: uma falha do sistema, acesso do atacante a falha que proporciona ao atacante explorar a falha.

> Vulnerabilidade são fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação: confidencialidade, integridade e disponibilidade. (CAMPOS, 2006, pág. 11)

Os principais ataques que estão relacionados a exploração de vulnerabilidade de tecnologia são os ataques ativos e ataques passivos:

- **Ataques Ativos e Ataques Passivos**

São ataques que prejudicam o fluxo normal da informação. Alterando o seu conteúdo e produzindo informação não válida, com intuito de violar a segurança de um sistema. Já os ataques passivos são ataques que não alteram a informação, nem seu fluxo normal, apenas ficam sob canal de escuta. (PINHEIRO, 2008)

Ameaças

É um evento indesejável que potencialmente desabilita, remove ou destrói algum recurso. As ameaças normalmente se aproveitam das falhas de segurança da organização. Há possibilidade de um agente ou fonte de ameaça explorar propositalmente uma vulnerabilidade específica. Segundo Campos (2006, p.13) a

ameaça é um agente externo ao ativo de informação, se aproveitando das vulnerabilidades da informação suportada ou utilizada por ele.

Riscos (externos e/ou internos)

De acordo com Pinheiro (2008), todo evento que possa causar impacto na capacidade de empresas atingirem seus objetivos de negócio. Probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização.

Formas de prevenção

Uma empresa de serviços de TI que protege seus clientes contra vazamento e perda de dados deve ter em um **gerenciamento proativo e preventivo**, agindo de forma a evitar que determinadas situações aconteçam.

Gerenciar riscos, com um monitoramento constante em busca de possíveis ameaças, faz parte da rotina de uma empresa de serviços de TI de sucesso. Muitos provedores de TI estão buscando no **MSP (Managed Service Provider)** um modelo de gestão baseado em prevenção, a fim de evitar situações-problema e, dessa forma, proteger os dados de seus clientes.

De acordo com o portal de notícias brasileiro G1 (2012), é importante ficar atento as políticas de privacidade, não divulgar dados pessoais e, em caso de perceber algo ameaçador é indispensável a denúncia pelo site: *https://new.safernet.org.br/denuncie/*.

A *SaferNet Brasil* oferece um serviço de recebimento de denúncias anônimas de crimes e violações contra os Direitos Humanos na Internet, contando com procedimentos efetivos e transparentes para lidar com as denúncias. Segundo o site, o tema com maior índice de denúncia é a de *pornografia infantil*, em segundo lugar *apologia e incitação de crimes contra a vida* e, em terceiro lugar o *racismo.* E de acordo com o gráfico retirado do site, as denúncias só aumentam. Por isso, é importante permanecer atento e denunciar sempre que for necessário.

CONCLUSÃO

A segurança da informação, portanto, é um fator primordial, que visa a segurança dos dados, a qualidade e a preservação, principalmente no meio organizacional. Durante o trabalho, foram apresentadas possíveis soluções para que determinados danos não aconteçam e prejudiquem qualquer organização, como o uso de softwares seguros e a manutenção que ocorre entre a circulação das informações organizacionais, visto que as informações têm seus riscos e vulnerabilidades.

Baseando-se nas pesquisas de Campos (2006), conclui-se que por parte das tecnologias da informação e seus profissionais, uma circulação de dados precisa produzir soluções convenientes às necessidades informacionais seguras e eficientes. A perspectiva deste artigo é de que todas as informações aqui citadas sejam como um manual, onde será possível encontrar as formas de preservação e conservação de dados e de como as vulnerabilidades surgem ao longo de uma informação.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002. **Código de prática para a gestão da segurança da informação.** Disponível em: <http://www.fieb.org.br/download/senai/nbr_iso_27002.pd f> Acesso em 19 dez. 2018.

CAMPOS, André L. N. **Sistema de Segurança da Informação: Controlando os riscos.** Florianópolis: Visual Books, 2006.

Canal Westcon. **Saiba quais são os 4 Princípios da Segurança da Informação** . Disponível em:<https://blogbrasil.westcon.com/saiba-quais-sao-os-4-principios-daseguranca- d a-informacao>. Acesso em: 13 dez. 2018.

FONTES, Edison. **Vivendo a segurança da informação: orientações práticas para pessoas e organizações.** São Paulo: Sicurezza, 2006.

Fundação Bradesco - Escola Virtual. **Segurança em Tecnologia da Informação**. Disponível em:<https://bit.ly/2rMbdZ d> . Acesso em: 18 dez. 2018.

GAZOLA, Rodrigo. **Entenda os principais riscos à segurança da informação.** Disponível em: <https://blog.addee.com.br/riscos-a-seguranca-da-informacao/> Acesso em: 18 dez. 2018

G1, Tecnologia e Games. **Safernet lança site que reúne denúncias de crimes na internet.** 2012**.** Disponível em:< http://g1.globo.com/tecnologia/noticia/2012/11/safernet-lanca-site-que-reune-de nuncias-de-crimes-na-internet.html>. Acesso em: 20 dez. 2018.

MOREIRA, Ademilson. **A importância da segurança da informação.** 2008. Disponível em: <http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao> Acesso em: 13 dez. 2018

OLIVEIRA, Waldes. **Riscos, vulnerabilidade e ameaça em Segurança da Informação.** Disponível em: <https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/> Acesso em: 18 dez. 2018

Política Segurança da Informação. **Raízen**. Disponível em:< https://www.raizen.com.br/sites/default/files/fornecedores_seguranca_da_informacao.pdf>.Acesso em: 12 dez. 2018.

PINHEIRO, Adriano. **A importância da Segurança da Informação - Tipos de ataques**. São Paulo, Maio 2008.

Segurança da Informação. **Segurança da Informação** . Disponível em:< http://seguranca-da-informacao.info/>. Acesso em: 11 dez. 2018.

TCU. **Boas Práticas na Segurança da Informação**. Disponível em:< http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 12 dez. 2018.