FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Gustavo De Souza Moraes

Patrick Allan Domingues Pereira

Segurança no comércio eletrônico

Americana, SP

2022

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

GUSTAVO DE SOUZA MORAES

PATRICK ALLAN DOMINGUES PEREIRA

SEGURANÇA NO COMÉRCIO ELETRÔNICO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Professor Me. Maxwel Vitorino da Silva.

Área de concentração: Criptografia.

Americana, SP

2022

Gustavo de Souza Moraes
Patrick Allan Pereira Domingues

SEGURANÇA NO COMERCIO ELETRÔNICO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Criptografia.

Americana, 07 de dezembro de 2022

Banca Examinadora:

Maxwel Vitorino da Silva (Presidente)
Mestre
FATEC Americana

Eduardo Antonio Vicentini (Membro)
Mestre
FATEC Americana

Maria Elizete Luz Saes (Membro)
Mestre
FATEC Americana

RESUMO

Com a evolução da internet no mundo todo o comércio eletrônico vem ganhando cada vez mais força, pois ele consegue alcançar um público abrangente e o mercado eletrônico está cada vez mais em ascensão. Entretanto, com essa evolução começa a aparecer pessoas mal-intencionadas para invadir a privacidade desses sites através de métodos que possibilitam entrar no computador do usuário sem que ele perceba e rouba dados confidenciais, prejudicando as empresas com roubo e vazamento de dados. Na segurança da informação há aspectos complexos como privacidade, autenticação e anonimato, essenciais para o comércio eletrônico. Confiabilidade e confidencialidade também são pré-requisitos muito importantes para o comércio eletrônico. Na pesquisa do trabalho foi utilizado uma abordagem qualitativa, ela pode ser definida como um estudo não estatístico, onde ocorre uma análise de dados sobre grupo de indivíduos mais subjetivo, não o ligando a algum problema em específico. A abordagem descritiva tem o objetivo de descrever as características do tema abordado, onde o assunto já é conhecido, mas visa proporcionar uma nova visão sobre ele. Essa monografia visa apresentar um estudo sobre a segurança, privacidade, e estratégias para se proteger de possíveis ataques no comércio eletrônico.

Palavras-chave: comércio eletrônico, segurança, privacidade.

ABSTRACT

With the evolution of the internet in the world, e-commerce is gaining more and more strength, as it manages to reach a wide audience and the electronic market is increasingly on the rise. However, with this evolution, malicious people begin to appear to invade the privacy of these sites through methods that make it possible to enter the user's computer without him detecting and stealing data, preventing companies with theft and data leakage. In information security, there are complex aspects such as privacy, login and anonymity, essential for electronic commerce. Reliability and confidentiality are also very important prerequisites for e-commerce. In the research work, a qualitative approach was used, it can be defined as a non-statistical study, where there is an analysis of data on a more subjective group of individuals, not linking it to any specific problem. The descriptive approach has the objective of describing the characteristics of the topic exactly, where the subject is already known, but it aims to provide a new vision about it. This monograph aims to present a study on security, privacy, and strategies to protect against possible attacks in electronic commerce.

Key words: e-commerce, security, privacy.

SUMÁRIO

LISTA DE FIGURAS

1. INTRODUÇÃO

A internet está em uma constante evolução, essa ferramenta vem evoluindo cada vez mais com o passar do tempo nos trazendo uma maior comodidade e rapidez nas nossas buscas.

Segundo O'Brien (2006) o crescimento explosivo da internet é um fenômeno revolucionário em computação e telecomunicações. Segundo O'Brien a internet está constantemente se expandindo, à medida que mais e mais empresas e outras organizações e usuários, aderem a essa rede mundial.

Por meio da internet o comércio de produtos de forma eletrônica ganhou um novo espaço, o espaço virtual, o que antes só dava para ser feito pelo meio tradicional, ou seja, por meio de loja física com clientes e vendedores reais, agora pode ser feito através de um celular ou computador, e não para por aí pode ser feito através de qualquer equipamento com acesso à internet.

De acordo com Laudon e Laudon (2007) não obstante, a Internet e o comércio eletrônico estão cada vez mais presentes no dia a dia das pessoas, possibilitando adquirir bens e serviços de maneira fácil e rápida.

Embora a maioria das transações ainda ocorra pelos canais tradicionais, um número crescente de consumidores e empresas estão usando a internet para fazer comércio eletrônico.

O mercado está em constante evolução e as empresas estão se adequando a um novo cenário de vendas que vem se expandindo cada vez mais com o passar dos anos, as empresas estão ficando mais flexíveis mantendo o comércio físico e eletrônico, cada vez mais estão olhando para fora em busca de novos clientes e o comércio eletrônico é uma boa saída.

A empresa mantém uma conexão privada com seus clientes, distribuidores, fornecedores e até com concorrentes. Essas conexões são chamadas de comércio eletrônico.

O comércio eletrônico é uma forma de realizar transações de compra e venda, as empresas publicam seus produtos em seus sites ou em site de terceiros para poder ser visto e avaliado por seus clientes e finalmente comprado, todo esse processo é feito de maneira virtual, ou seja, por meio eletrônico.

De acordo com Laudon e Laudon (2007) comércio eletrônico ou (*e-commerce*) refere-se ao uso da Internet e da Web para comercializar mercadoria e serviços. Diz

respeito às transações comerciais realizadas digitalmente entre organizações e indivíduos ou entre duas, ou mais organizações.

Apesar de toda comodidade que esse método nos dá, muitas pessoas não confiam por receio das ameaças que a internet pode trazer quando exercitamos essa modalidade comercial, por exemplo, as ameaças que existem na internet, falta de conhecimento, violação, roubo e troca de dados dos usuários.

Por conta dessas ameaças, o consumidor precisa sempre verificar se o site que deseja realizar a compra possui meios de seguranças que evita terceiros ter acesso a dados confidenciais. Vale ressaltar que o comércio eletrônico está voltado não só para consumidores, mas também para as empresas. Umas das opções de segurança que existe e pode ser usada é uma técnica desenvolvida chamada criptografia.

Para a pesquisa desse trabalho foi utilizado uma abordagem qualitativa, que pode ser definida como um estudo não estatístico, onde ocorre uma análise de dados sobre grupo de indivíduos mais subjetivo, não o ligando a algum problema em específico, na abordagem descritiva ela tem o objetivo de descrever as características do tema abordado, onde o assunto já é conhecido, mas visa proporcionar uma nova visão sobre ele.

Esta monografia tem por objetivo apresentar um estudo sobre a segurança, privacidade, estratégia para se proteger de possíveis ataques e descrever as técnicas utilizadas pelo comércio eletrônico para proporcionar uma melhor segurança como a Criptografia, o Site Blindado e a Assinatura Digital.

2. *E-COMMERCE*

O *e-commerce* vem crescendo muito com o passar dos anos, hoje é uma forma muito comum e prática de efetuar suas comprar. O *e-commerce* se trata de uma loja virtual onde as empresas colocam seus catálogos de venda, e com poucos seus clientes podem efetuar a compra de um produto sem precisa sair de casa.

Segundo Laudon e Laudon (2004, pg. 180):

> "O comércio eletrônico é o processo de compra e venda de produtos eletronicamente. Pela automatização das transações de compra e venda, as empresas podem reduzir seus procedimentos manuais e baseados em papel e acelerar pedidos, entrega e pagamento de produtos e serviços."

Por conta da praticidade desse tipo de comércio, ele vem crescendo muito, é cada vez mais comum a prática de compras online, mas onde isso começou?

Os primeiros indícios do e-commerce foi 1970, nos Estados Unidos, onde ocorria como troca de arquivos de solicitação de pedidos. Enquanto no Brasil, o primeiro registro de e-commerce foi em 1996, o conceito de e-commerce ainda era muito desconhecido, porém ganhou mais força em 1999 com o surgimento Submarino, uma das pioneiras de vendas online.

Com o passar dos anos essa área foi crescendo muito, mas seu índice de crescimento aumentou muito com o surgimento da pandemia, no começo de 2020.

A pandemia teve um grande impacto no comércio eletrônico brasileiro. Pesquisa feita pela Federação Getúlio Vargas (FGV) apontam que antes da pandemia as vendas online no cenário do e-commerce brasileiro correspondiam a 9,2% das receitas, porém, em julho de 2020 esse número subiu para 19,8%, em apenas 4 meses de pandemia já teve um grande aumento, e em julho de 2021, esse número subiu para 21,2%.

Outros dados que mostram esse crescimento é que antes da pandemia, 49,7% das empresas não faziam vendas online, e com o fechamento das lojas físicas, o porcentual caiu para 20,2% em julho de 2021, isso mostra o grande aumento do comércio eletrônico e a importância e necessidade dessa área na economia brasileira, principalmente em época de pandemia.

Os números levantados pelo FGV realmente mostram o impacto do e-commerce da sociedade. Segundo Tobler (2021) o resultado confirma-se por meio de

análise numérica a hipótese de que as empresas aceleraram o processo de digitalização ao longo da pandemia, principalmente para minimizar os impactos negativos da queda de circulação de pessoas nas lojas físicas.

3. SEGURANÇA DAS INFORMAÇÕES EM TRANSAÇÕES ELETRÔNICAS

A segurança nas transações eletrônicas é um ponto de muita desconfiança por parte dos consumidores, preocupado com os dados e sigilo de suas informações como nome, e-mail, telefone, endereço, etc., alguns clientes ficam com receio de passar esses dados sensíveis por medo de ocorrer algum vazamento ou que esses dados sejam alterados por algum “terceiro”.

A falta de confiança dos consumidores é um dos pontos a ser levantado, isso acontece desde quando surgiu essa modalidade de comércio. Existe uma certa percepção na cabeça dos consumidores que a rede de computadores está sujeita a constantes ataques, embora essa percepção seja exagerada é necessário levar em consideração.

A facilidade que empresas virtuais são criadas e conseguem vender seus produtos pelo mundo é bem grande, pensando nisso é bem fácil uma empresa ser criada e após transacionar algum produto para o consumidor ela pode simplesmente deixar de existir depois e recolher o seu dinheiro.

Essas preocupações são geradas por conta dos crackers infratores virtuais que consegue driblar sites com extrema segurança, basta ter alguma brecha, até conseguir ter acesso a dados pessoais dos clientes como: número do cartão de crédito, número da conta-corrente, e-mails e senhas. Tendo essas informações em mãos é possível fazer operações como, fazer transferência de valores e espionar informações, dentre outras.

Segundo Turban e King (2004, pg. 312):

> “O consumidor deve ser notificado sobre a prática de informações de uma entidade antes da coleta de informações pessoais. Também deve poder tomar decisões sobre o tipo e a extensão da divulgação das informações, com base as intenções da parte que as está coletando. O consumidor deve poder acessar suas informações pessoais e contestar a validade dos dados. Deve-se garantir aos consumidores que seus dados pessoais estão seguros e são exatos. Quem coleta os dados deve tomar todas e quaisquer preocupações exigidas para garantir que os dados estejam protegidos contra perda, acesso não autorizado, destruição e utilização fraudulenta, além de tomar as providências razoáveis para obter informações de fontes respeitáveis e confiáveis. Deve sempre existir um método de cumprimento e recurso. Caso contrário, não haverá nenhum impedimento real ou obrigatoriedade de cumprimento para as questões de privacidade. As

> alternativas são a intervenção governamental, a legislação para recursos privados ou a autorregulamentação.”

A segurança tem se aprimorado com o tempo, pois o interesse é uma via de mão dupla, tanto o consumidor como o vendedor vão se beneficiar disso quanto mais confiança o consumidor ter em comprar por essa modalidade vai ser benéfico para ele fazer compras com facilidade e no conforto de sua casa, deve se garantir a segurança na internet através de alguns conceitos como: confidencialidade, integridade, autenticação e não repudio.

O conceito de confidencialidade deve garantir que o conteúdo das informações das transações feitas por meio eletrônico seja protegido de pessoas que não estão autorizadas a recebê-las. Deve se manter o sigilo de todas as informações importantes como: número da conta, cartões, documentos e valor da compra.

De acordo com Dias (2000) ao ocultar a informação, por meio do texto cifrado proporciona confidencialidade. Ao mesmo tempo, garante a integridade de dados, pois o conteúdo da mensagem fica inalterado desde a cifragem até a decifragem.

A autenticação vai ser o processo responsável por identificar usuários, nesse caso deve garantir a autenticidade mútua. Assim vai ser garantido que a informação que está se passando seja entregue para o destinatário correto e não para um impostor, e que a mensagem que o destinatário vai receber seja a original.

Beal (2005) afirma que alguns autores acrescentam a esses três requisitos, o da legalidade (garantia de que a informação foi produzida conforme a lei), ou ainda o de “uso legitimo” (garantia de que os recursos de informação não são usados por pessoas não autorizadas ou de maneira não autorizada).

Para ser compreendido o significado de não repudio, é necessário que o tema seja definido.

Para Lara (2006) O repúdio é o fato de se negar a participação numa determinada operação. O problema realmente surge se a negativa, ou seja, o repúdio, acontecer sobre uma operação que de fato ocorreu.

No comércio virtual, assim que é realizado a transação, tanto o comprador como o vendedor não podem negar participação na mesma, independente da modalidade de comércio eletrônico.

4. MODALIDADES DE COMÉRCIO ELETRÔNICO

Pode-se distinguir várias modalidades no comércio eletrônico, tais como: *Businessto-Business*(B2B), *Business-to-Consumer*(B2C), *Business to Government*(B2G), *Government to Consumer*(G2C) e *Consumer to Consumer*(C2C), as quais podem ser definidas da seguinte forma:

4.1. *Businessto-Business*-B2B (NEGÓCIO-A-NEGÓCIO)

Este é dito ser o setor do comércio eletrônico em mais rápido crescimento. A previsão é que o modelo B2B se torne o setor de maior valor da indústria dentro de alguns anos. O modelo B2B envolve transações eletrônicas para encomendas, compras, bem como outras tarefas administrativas entre casas. Ele inclui o comércio de bens, tais como assinaturas de negócios, serviços profissionais, manufatura e negociações no atacado.

Por vezes, no modelo B2B, os negócios podem existir entre empresas virtuais, nenhuma das quais pode ter qualquer existência física. Nestes casos, os negócios são conduzidos apenas através da Internet. As duas principais vantagens do modelo B2B, tais como a possibilidade de manter eficientemente o movimento da cadeia de fornecimento e os processos de fabricação e de produção, e pode automatizar os processos corporativos para entregar os produtos e serviços certos de forma rápida e eficaz em termos de custos.

Segundo Mendes (2011) em 2005, de acordo com a revista Info Exame, foi movimentado 67 bilhões de dólares no comércio eletrônico brasileiro. Apenas a Petrobrás foi responsável por 45 bilhões de dólares com B2B.

4.2. *Business-to-Consumer*-B2C (NEGÓCIO-A-CLIENTE)

O modelo B2C envolve transações entre organizações empresariais e consumidores. Aplica-se a qualquer organização empresarial que venda os seus produtos ou serviços aos consumidores através da Internet. Estes sites exibem informações sobre os produtos num catálogo online e armazenam-nas numa base de dados.

O modelo B2C também inclui serviços bancários online, serviços de viagens e informação sobre saúde. O modelo B2C de comércio electrónico é mais propenso às ameaças à segurança porque os consumidores individuais fornecem o seu cartão de crédito e informação pessoal no site de uma organização empresarial.

Além disso, o consumidor pode duvidar que suas informações estejam seguras e sejam utilizadas de forma eficaz pela organização empresarial. Esta é a principal razão pela qual o modelo B2C não é muito bem aceito.

Portanto, torna-se muito essencial para as organizações empresariais fornece mecanismos de segurança que possam garantir ao consumidor a segurança da informação empresarial.

4.3. *Consumer-to-Consumer*-C2C (CONSUMIDOR-PARA-CONSUMIDOR)

O modelo C2C envolve transações entre consumidores. Aqui, um consumidor vende diretamente a um outro consumidor. Os sites de leilões on-line que fornecem a um consumidor para anunciar e vender os seus produtos online a outro consumidor. No entanto, é essencial que tanto o vendedor como o comprador se registem no site do leilão.

Enquanto o vendedor precisa pagar uma taxa fixa à casa de leilões online. Se o comprador se deparar com tal produto, ele coloca um pedido para o mesmo no site do *eBay*. A *EBay* compra agora o produto junto ao vendedor e depois vende ao comprador. Desta forma, embora a transação seja entre dois clientes, uma organização atua como uma interface entre as duas organizações.

4.4. *Consumer-to-Business*-C2B (CONSUMIDOR-PARA-EMPRESA)

Modelo *Consumer-to-Business* (C2B) O modelo C2B envolve uma transação conduzida entre um consumidor e uma organização empresarial. É semelhante ao modelo B2C, porém, a diferença é que neste caso o consumidor é o vendedor e a organização de negócios é o comprador. Neste tipo de transação, os consumidores decidem o preço de um determinado produto e não o fornecedor.

Além dos modelos discutidos até agora, estão sendo trabalhados cinco novos modelos que envolvem transações entre o governo e outras entidades, tais como consumidores, organizações empresariais e outros governos. Todas essas

transações que envolvem o governo como uma entidade única são chamadas de governança

Os vários modelos no cenário de *E-Governance* são:

a) Modelo *Government-a-Government* (G2G): Este modelo envolve transações entre 2 governos. Por exemplo, se o governo indiano quiser comprar petróleo do governo árabe, as transações envolvidas são categorizadas no modelo G2G.

b) Modelo *Government-Consumer* (G2C): Neste modelo, o governo transaciona com um consumidor individual. Por exemplo, um governo pode aplicar leis relativas a pagamentos de impostos de consumidores individuais pela Internet usando o modelo G2C.

c) Modelo *Consumer-to-Government* (C2G): Neste modelo, um consumidor individual interage com o governo. Por exemplo, um consumidor pode pagar seu imposto de renda ou casa taxa online. As transações envolvidas neste caso são transações C2G.

d) Modelo *Government-to-Business* (G2B): Este modelo envolve transações entre organizações governamentais e empresariais. Por exemplo, o governo planeja construir um viaduto. Para isso, o governo solicita licitações de várias empreiteiras. O governo pode fazer isso pela Internet usando o modelo G2B.

e) Modelo *Business-to-Government* (B2G): Neste modelo, as casas de negócios transacionam com o governo pela Internet. Por exemplo, semelhante a um indivíduo consumidor, casas de negócios também podem pagar seus impostos na Internet.

Benefícios do *E-Commerce* para os negócios:

a) Mercado Internacional - O que costumava ser um único mercado físico localizado em uma área geográfica tornou-se agora um mercado sem fronteiras, incluindo nacional e mercados internacionais. Ao tornarem-se habilitados para comércio eletrônico, as empresas agora têm acesso apessoas em todo o mundo. todos os negócios de comércio eletrônico se tornaram virtuais corporações multinacionais.

b) Economia de custos operacionais - O custo de criação, processamento, distribuição, armazenamento e recuperação de informações em papel diminuiu.

c) Customização em massa - O comércio eletrônico revolucionou a forma como os consumidores compram mercadorias e serviços. O processamento permite que produtos e serviços sejam customizados para os requisitos do cliente. No passado, quando a Ford começou a fabricar automóveis, os clientes poderiam ter qualquer cor, desde que fosse preto. Agora os clientes podem configurar um carro de acordo com suas especificações dentro de minutos on-line através do site da Ford.

d) Menor Custo de Telecomunicações - A Internet é muito mais barata do que as redes de valor acrescentado (VANs) que se baseavam no aluguer de linhas telefónicas para uso da organização e dos seus parceiros autorizados. Também é mais barato enviar um fax ou e-mail através da Internet do que discar diretamente.

e) Digitalização de Produtos e Processos - Especialmente no caso de software e produtos de música/vídeo, este pode ser descarregado ou enviado diretamente aos clientes através da Internet em formato digital ou eletrônico.

f) Acabaram-se as restrições de 24 horas - As empresas podem ser contactadas por clientes ou fornecedores os contatos em qualquer altura.

Benefícios do *E-Commerce* para os Consumidores:

a) Acesso 24/7 - Permite aos clientes fazer compras ou realizar outras transações 24 horas, durante todo o ano, a partir de quase todos os locais. Por exemplo - verificação de saldos, realização de pagamentos, obtenção de viagens e outras informações.

b) Mais escolhas - Os clientes não só têm toda uma gama de produtos que podem escolher e personalizar, mas também uma seleção internacional de fornecedores.

c) Comparações de Preços - Os clientes podem "fazer compras" em todo o mundo e realizar comparações diretamente visitando diferentes sites, ou visitando um único site onde os preços são agregados a partir de um número de fornecedores e comparados. Processos de Entrega Melhorados - Pode variar desde a entrega imediata de mercadorias digitalizadas ou eletrônicas, tais como software ou ficheiros audiovisuais por download via Internet, até ao acompanhamento on-line do progresso das embalagens a serem entregues por correio.

e) Um Ambiente de Concorrência - Onde podem ser encontrados descontos substanciais ou valor acrescentado, uma vez que diferentes retalhistas disputam com os clientes. Também permite a muitos clientes individuais agregar as suas encomendas numa única encomenda apresentada a grossistas ou fabricantes e obter um preço mais competitivo.

Benefícios do *E-Commerce* para a Sociedade:

a) Possibilita Práticas de Trabalho mais Flexíveis - Isto melhora a qualidade de vida de toda uma série de pessoas na sociedade, permitindo-lhes trabalhar a partir de casa. Isto não só é mais conveniente e proporciona ambientes de trabalho mais felizes e menos estressantes, como também reduz potencialmente a poluição ambiental, reduzindo o número de pessoas que têm que viajar regularmente para trabalhar.

b) Conecta Pessoas - Permite que as pessoas nos países em desenvolvimento e áreas rurais desfrutem e tenham acesso a produtos, serviços, informações e outras pessoas que de outra forma não estariam tão facilmente disponíveis para elas.

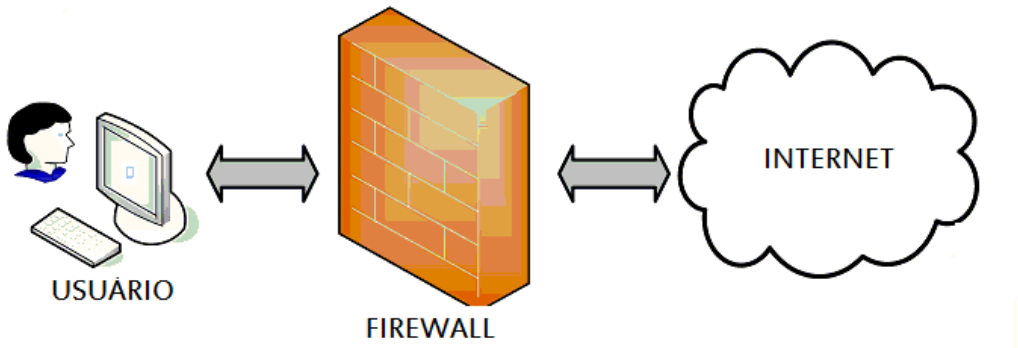
c) Facilita a Prestação de Serviços Públicos - Por exemplo, serviços de saúde disponíveis através da Internet (consulta on-line com médicos ou enfermeiros), arquivando impostos através da Internet através do site da Receita Federal

5. *FIREWALL*

O *Firewall* é um sistema ou grupo de sistema que aplicam políticas de controle de acesso entre duas redes. Ao navegar pela internet você fica exposto a vários riscos de segurança, pois nela há vários sites ou links maliciosos.

O *Firewall* serve como uma barreira que fica entre a rede interna da empresa (rede segura) e a internet externa (rede não confiável), e essa barreira filtra as informações e protege a rede interna de possíveis ameaças externas, como mostra a Figura 1.

Figura 1: *Firewall*.



Fonte: Hardtech, 2021.

Esse controle e filtragem dos dados de redes é feita de acordo com regras pré-estabelecidas, chamamos essas regras de “Política de Segurança”.

Segundo Filho (2002), o *firewall* é um dispositivo de hardware e software que tem como principal função filtrar pacotes na rede, visando proteger, negando informações ou repassando comunicações a respeito do evento.

Ele pode ser implementado de várias maneiras, como limitando acesso de certas aplicações ou limitando a quantidade de pessoas autorizadas a certa aplicação, entre outros. Segundo Kurose e Ross (2006) o *firewall* permite a um administrador de rede controlar o acesso entre o mundo externo e os recursos da rede que ele administra, gerenciando o fluxo de tráfego de e para esses recursos.

Esse controle ou restrição de informações pode tornar a empresa mais segura, porém também pode trazer algumas desvantagens, ente elas, a restrição de acesso pode também limitar as operações relacionadas a publicidade, compra e venda de produtos.

Para diminuir essas desvantagens normalmente opta-se por utilizar um sistema de *firewall* com poucas restrições no momento de realizar essas atividades de publicidade, compra e venda, e quando a empresa precisar partilhar arquivos e informações confidenciais pode-se aumentar a restrição de acesso alterando as configurações do *firewall*.

Várias informações podem ser barradas pelo *firewall*, porém há ameaças que o ele não consegue proteger as máquinas, elas são:

- Ataques que atravessam ele, chegando na rede interna;
- Ameaças internas, como funcionários;
- Infecções de vírus e outros tipos de *malwares*, principalmente entre máquinas na rede interna.

Segundo Kurose e Ross (2006) os *firewalls* podem ser classificados em três categorias: filtros de pacotes tradicionais, filtros de estado e gateways de aplicação. A seguir será abordado as três categorias.

5.1. Filtro de pacote

De acordo com Kurose e Ross (2006, p. 539), o filtro de pacote tem a função de examinar toda a rede e determinar quais dados podem passar e quais devem ser bloqueados se baseando em regras definidas pelo administrador.

Irá ser feita a análise dos pacotes e identificação das informações em seu cabeçalho, se alguma das informações do pacote for congruente com a primeira regra, ela será aplicada e as demais regras serão ignoradas, caso ao contrário, ele irá conferir regra por regra até que alguma possa ser aplicada para determinado pacote.

Conforme Kurose e Ross (2006, p. 539), as regras de filtragem são baseadas no conteúdo do pacote, como IPs de origem e destino, nº de portas de comunicação, tipo de protocolo, interface de rede, entre outros.

Caso nenhuma regra possa ser aplicada no pacote, é aplicada uma regra padrão, podendo ser essa “Descartar (*Drop, Block, Deny*)” ou “Permitir (*Allow*)”.

Segue imagem de exemplificação:

Figura 2: Filtro de pacote.

Fonte: Erika Hoyer, et al, 2013.

Assim como todos os tipos de segurança, o filtro de pacote não é perfeito, ele apresenta alguns problemas e desvantagens, são essas:

- Não são efetivos contra-ataques que explorem vulnerabilidades das aplicações, por conta de agir nas camadas 3 e 4 da OSI, não examinando camadas superiores;
- Não suporte esquemas de autenticação de usuários;
- Pode ser facilmente falsificado, pois não verifica a carga útil.

5.2. Filtro de Estado de Sessão

Esse tipo de *firewall* é basicamente um aprimoramento do tipo anterior, porém, ao invés de analisar todos os pacotes recebidos, ele irá examinar a condição das conexões ativas, isso desde o começo até o final desta conexão.

Após essa análise, o *firewall* irá determinar se a conexão estabelecida é segura ou não, e então irá permitir ou bloquear o tráfego conforme o estado.

De acordo com Lima e Geus (1999), “um filtro de pacotes com estados geralmente pode implementar um *proxy* mais simples no kernel do sistema operacional e, em simultâneo, funcionar como um filtro de pacotes tradicional”.

5.3. Gateway de aplicação (*Proxy*)

O servidor *Proxy* é um intermediário na comunicação dos computadores de uma rede interna com a internet.

Segundo Lima e Geus (1999) “Um *proxy*, na verdade, evita que hosts na rede interna sejam acessíveis de fora da rede protegida, usando duas conexões: uma entre o cliente e o servidor proxy e outra entre o servidor *proxy* e o servidor real”.

Esse servidor também é chamado de procurador, pois é por meio dele que o cliente tem acesso a outros servidores na internet, ou seja, o cliente, ao fazer uma requisição de acesso a determinado link/servidor, essa requisição irá primeiramente para o servidor *proxy*, o qual fará uma análise da requisição e solicitará acesso a estes recursos em outros servidores.

De acordo com Souza (2013) “o *proxy* permite fazer o controle de acesso à Internet de acordo com a política de controle estabelecida pela empresa”.

Essa função é muito usada em ambientes empresariais e principalmente escolares. Nesses ambientes, algumas instituições acham desnecessário o acesso a certos sites, como redes sociais particulares, e por isso acabam bloqueando o acesso à essas páginas.

Outra função do servidor *proxy* que é muito utilizada é limitação de acesso. Muitas escolas, faculdades, empresas ou estabelecimentos que possuem conexão Wi-Fi, implementam um sistema de login ou senha para que o uso da internet não seja feito pela vizinhança, até onde o sinal é captado, o que pode causar lentidão na conexão.

6. S_HTTP

O S_HTTP (*Secure Hyper Text Transfer Protocol*) é uma extensão para o HTTP, esse protocolo permite a troca de dados na internet de forma segura. Ele traz a possibilidade de várias opções de segurança por meio da comunicação entre servidor e cliente, providenciando integridade, autenticação, confidencialidade e certificação.

Segundo LAUDON e LAUDON (2001) Para ser lida, a mensagem precisa ser descriptografada (desembaralhada) com uma chave de combinação. “Existem vários padrões de criptografia, entre eles o SSL (*Secure Sockets Layer*) e o S-HTTP (*Secure Hypertext Transport Protocol*), os quais são usados para o tráfego baseado na Web.”

O tópico seguinte irá demonstrar a função e importância da criptografia na segurança da informação.

7. Criptografia

A criptografia é usada há muitos anos, ela era normalmente utilizada para comunicações sigilosas em guerras. O primeiro documento de criptografia encontrado é de 1900 A.C., no Egito

Segundo Ferreira (2003), a criptografia nasceu da necessidade de manter a privacidade das informações. Desde a antiguidade já se tinha conhecimento da criptografia onde era utilizada a substituição ou a troca de símbolos visando confundir um possível interceptador das mensagens.

Segundo Ferreira (2003) Na computação esse princípio é mantido, porém, a escrita é substituída pelo processamento digital da informação e com a capacidade de processamento de dados desta tecnologia.

Para Veloso (2002) A criptografia é algo essencial para se realizar transações eletrônicas seguras. Porém, ao ser apresentado o número do cartão de crédito pode levar o proprietário a ser fraudado, tendo o seu número de cartão de crédito usado sem sua autorização.

A encriptação se trata da transformação de dados de uma forma que não possa ser lida, ela tem o propósito de assegurar a privacidade da mensagem e que seja lida apenas para a quem for destinada, mesmo aqueles que podem tê-la encriptado. A decriptação é o oposto da encriptação: é a transformação dos dados encriptados de volta para uma maneira inteligível.

Para Veloso (2002) Mecanismos de transação segura são usados na Internet, onde o número do cartão é enviado com outras informações de forma encriptada, permitindo assim que o pagamento seja feito de forma segura.

Isso permite que, por exemplo, consumidores e vendedores troquem informações de forma segura, dificultando o acesso de pessoas que não possui boas intenções, garantido que elas não consigam roubar os dados.

Para fornecer mais segurança aos seus clientes ao fornecer dados transmitidos pela rede, existe três serviços de criptografia:

- Confidencialidade: Todas as normas e ações inclusas nesse pilar visam proteger os dados de quem não deve ter acesso a eles. Uma das ações dessa área é a implementação de criptografia nos dados e controle de acesso às informações.
- Integridade: Esse pilar tem o objetivo de garantir que as informações não sejam alteradas no caminho de seu destino, ou seja, que ela seja recebida e

visualizada da mesma maneira que foi encaminhada, sem modificações em seu conteúdo

- Autenticidade: Garantir que a fonte das informações seja confiável, para isso é preciso manter um registro de autor, assim é possível determinar a veracidade da informação.

Um dos primeiros métodos que apareceu na criptografia se chama: cifra de substituição e transposição. O primeiro deles substitui cada letra ou um grupo de letras por alguma letra, ou um conjunto de letras, as letras passam por modificações, mas a ordem não muda, já na cifra de transposição troca os caracteres do mesmo texto, de posição. Os dois métodos são fáceis de ser decifrados quando se sabe das regras.

A criptografia é um método bem antigo como dito anteriormente, hoje é muito mais eficiente do que nos tempos passados, ela passou por diversas melhorias com o passar do tempo, com seu grande crescimento e uso diário sugiram dois novos tipos de criptografia: simétrica e assimétrica, que vai ser mostrado mais adiante. Ambas funcionam através do conceito de chaves.

A utilização de chaves é um método bem mais seguro do que os algoritmos, pois no uso do algoritmo, alguma pessoa mal-intencionada pode decifrar e ver todos seus dados, utilizando o método de chaves cada informação pode ter uma chave, sendo assim mesmo que alguém tenha acesso à determinada chave as outras informações estarão seguras.

As chaves são calculadas através dos números de bits, tais como: 8, 64, e 128 bits, etc. Por exemplo: se uma chave corresponde a um valor de 8 bits, esse valor deverá ser elevado ao quadrado, ou seja, 8^2, no qual o resultado será igual a 256. Esse valor vai representar a quantidade de possíveis decodificações, sendo um valor baixo que pode ser decifrado facilmente por alguém que tenha tempo e fique tentando diversas combinações, com isso conseguimos concluir que quanto maior for o número de bits, maior será a segurança da Criptografia.

Este é o conceito de chaves, esse processo visa impedir que o texto seja lido por terceiros que poderiam ter interceptado a mensagem no meio do caminho. A seguir vemos os dois métodos de criptografia, a criptografia simétrica e assimétrica.

7.1. Criptografia simétrica

É a mais comum das criptografias, conhecida como criptografia chave privada ou chave secreta. Está é a técnica que utiliza apenas uma chave, sendo que o emissor vai usá-la para cifrar e o receptor para decifrá-la.

De acordo com Burnett (2002) a criptografia de chave simétrica utiliza a mesma chave para cifragem e decifragem. Então, a chave deve ser conhecida tanto pelo emissor quanto pelo destinatário da mensagem.

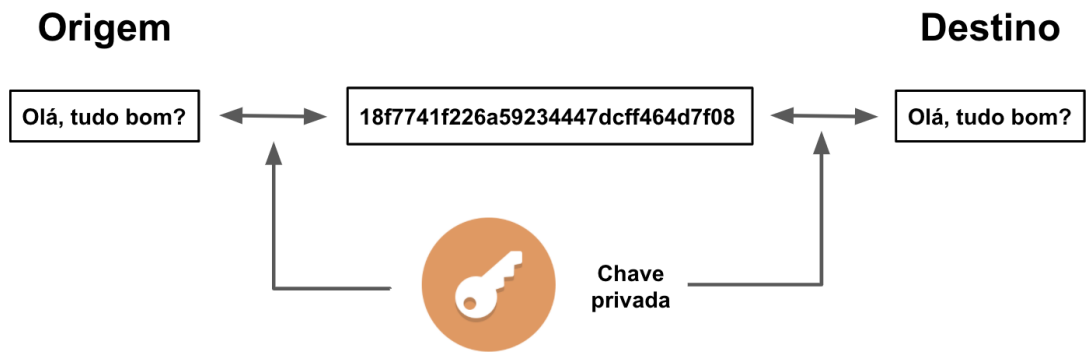
E para conseguir concretizar a transmissão da mensagem. Tanto o emissor quanto o receptor devem possuir o algoritmo da mensagem. Mesmo que algum intruso conheça o algoritmo da mensagem, ele não conseguira decifrar a mensagem. Sem possuir a chave.

Uma desvantagem dessa técnica, é que ambas as partes vão receber a mesma chave e assim aumenta e muito a chance da quebra das informações enviadas, sendo assim caso o intruso consiga pegar alguma das chaves ele conseguira fazer o que quiser com a informação armazenada por essa chave, sendo um risco grande para quem utiliza esse método.

Para Burnett (2002) a maior dificuldade do método é a distribuição segura das chaves. Em um sistema criptográfico de chave simétrica, a chave é apenas um número qualquer que tenha um tamanho correto, e que o selecione aleatoriamente.

O processo de chave simétrica poderá ser visualizado no exemplo da Figura 3, onde a chave privada está sendo usada para criptografar o texto e para descriptografar.

Figura 3: Chave Simétrica.



Fonte: Universidade Java, 2020.

7.2. Criptografia assimétrica

Outro método que é muito conhecido é a criptografia assimétrica, ou como também é conhecida chave pública, esse método trabalha com um par de chaves, sendo ela as: públicas e privadas.

Em 1976 foi proposto pela dupla Diffie e Hellman, a criptografia de chave pública ou chave assimétrica, com a proposta de chave assimétrica, o problema de segurança da chave seria resolvido.

O sistema de criptografia assimétrica pode fazer o uso de assinatura digital que vai autenticar o emissor. Pois apenas o emissor, o proprietário, vai fazer o uso exclusivo de sua chave privada, constando nela o seu documento e a sua assinatura digital, sendo assim, o nosso destinatário consegue verificar de quem veio a mensagem através de sua chave pública disponibilizada pelo proprietário.

Segundo Alecrim (2011) a Assinatura digital faz parte da função *hash* junto ao documento a ser enviado e na utilização das chaves criptográficas. No procedimento de conferência, deve-se calcular o *hash* e decifrar as chaves criptográficas, onde qualquer alteração nos dados, resultará em um resumo diferente, constatando ocorrência de adulteração das informações.

A vantagem da criptografia assimétrica é a utilização de duas chaves que vão servir, para encriptar e decriptar as informações, sendo assim dela poderá ser a privada, que o proprietário utilizou para fazer a encriptação das informações. Diante disso, somente a chave pública poderá decripta-las, ou vice-versa, sendo este o método mais seguro. Onde o proprietário vai conseguir manter as informações em sigilo e uso exclusivo dele.

Para Burnett (2002) a grande vantagem deste método é a segurança, pois não é necessário compartilhar a chave privada. Em contrapartida, o tempo de processamento de mensagens com criptografia assimétrica é muito maior do que com criptografia simétrica, o que pode limitar seu uso em algumas situações.

Diferente da chave simétrica que pode criptografar e descriptografar um arquivo, com a chave assimétrica será usado a chave pública para criptografar um arquivo e vai enviar ele para quem possui a chave privada, porque somente com a chave privada será possível descriptografar o arquivo.

O processo da chave assimétrica é visualizado na Figura 4:

Figura 4: Chave assimétrica.

Fonte: Universidade Java, 2020.

A garantia de que a criptografia do site é segura é confirmada pela instituição Site Blindado S/A.

8. Site blindado

A empresa site blindado S/A, fundada em 2005, é especializada em segurança na web. A empresa emite uma certificação de (selo site blindado), ela garante maior segurança “blindagem” de lojas virtuais, passando mais confiança para os clientes na hora de pôr informações pessoais como número de cartão de crédito para finalizar a compra.

A figura 5 apresenta o selo para o site blindando.

Figura 5: Site blindado.

Fonte: Logo Vector Seek, 2021.

Segundo Renkel (2021), a blindagem de sites funciona da seguinte maneira, é feito diversos scans durante o dia em busca de vulnerabilidades que comprometa a segurança do negócio, caso encontre alguma brecha o site corrigi a vulnerabilidade, quando o site passar por todos esses testes ele pode usar o selo de blindagem, qualquer usuário pode clicar no selo de blindagem do site e ver a auditoria feita no site passando mais confiança para seus clientes.

Hoje em dia diversas lojas de varejo utiliza o selo site blindado, lojas como americanas, submarino, ultrafarma dentre outras.

No momento de transação eletrônica entre as contas do comprador e do vendedor é usado o protocolo SET, o qual será mostrado a seguir.

9. SET

O SET (*Secure Electronic Transaction*) é um protocolo usado no uso de cartões de crédito para compras de produtos pela internet. O SET tem o objetivo de entregar segurança para as informações pessoais e bancárias do comerciante e comprador envolvidos no negócio, provendo confidencialidade, integridade, autenticação do titular do cartão e do comerciante.

Segundo Albertin (2001) o SET estabelece um padrão único para proteger as compras com cartão realizadas pela internet e em outras redes abertas. Os objetivos da segurança de pagamento são: prover autenticação dos portadores de cartão, vendedores e adquirentes; prover confidencialidade dos dados de pagamento; preservar a integridade dos dados de pagamento; e definir os algoritmos e protocolos necessários para esses serviços de segurança.

O SET não é o sistema que vai permitir que o pagamento seja feito, mas vai garantir que a transação seja segura, no SET é usado diferentes técnicas de criptografia e *hash* para manter a segurança dos cartões de crédito, este protocolo obteve apoio de grandes empresas como VISA e Mastercard.

O protocolo SET restringe para os comerciantes os detalhes do cartão na hora da compra, isso permite uma maior segurança e garante que ladrões e crackers ficaram longes.

Sua primeira versão foi lançada em 31 de maio de 1997, e a segurança desse sistema tem como processo a troca de dados criptografados durante toda a comunicação feita entre cliente e servidor, nas atividades de autorização, autenticação e identificação.

Essa comunicação entre cliente e servidor envolvem outros participantes, os quais vão ser descritos abaixo.

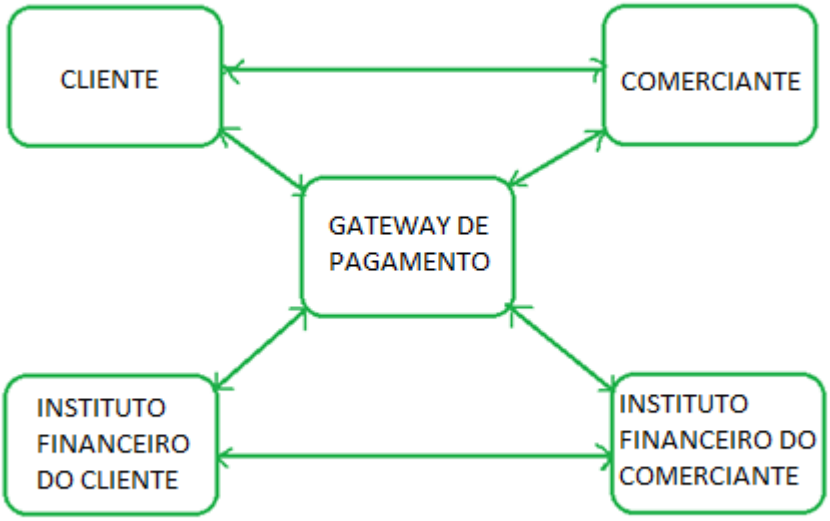
9.1. Participantes do SET

- Comprador
- Vendedor
- Empresa bancária responsável pelo cartão do comprador
- Empresa bancária ligada com o vendedor
- Gateway de pagamento (exemplo: cartão master/cartão visa)

- Autoridade de certificação (autoridade que emite certificados para todos os participantes).

A Figura 6 mostra todos os participantes do SET e demonstra como todos estão ligados ao Gateway para que a comunicação entre eles seja feita:

Figura 6: Participantes do SET.



Fonte: Geeks for Geeks, 2021.

9.2. Gateway de pagamento

Em um cenário geral de transação eletrônica, possui algumas etapas, como o gateway de pagamento, o sistema responsável por conectar e transferir os dados de forma rápida e com mais segurança do cliente para a instituição financeira, como operadoras de cartão e bancos.

Ele é um dos pilares mais importantes se tratando de lojas virtuais, pois se não tiver essa plataforma o cliente não consegue efetuar a compra online, é indispensável ter uma plataforma como essa que permita o pagamento no ato da compra.

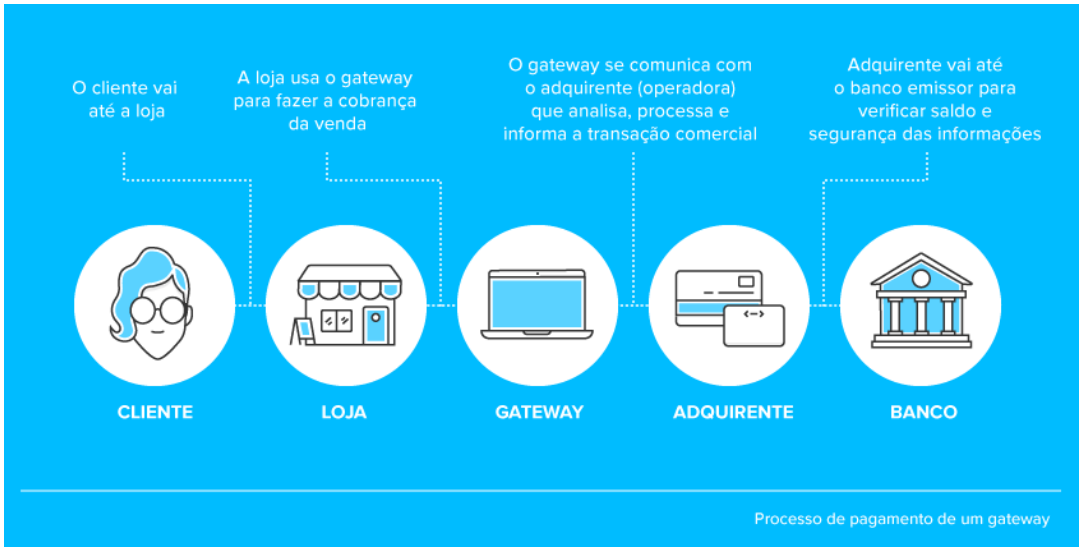
Além disso, através do gateway o lojista consegue oferecer ao seu cliente diversas formas de pagamento, como a mais popular hoje em dia que é o pix, ou pagar com cartão de crédito, débito e até mesmo o boleto.

De maneira geral o gateway vai permitir que o cliente no ato da compra consiga selecionar a forma de pagamento, através disso o valor da compra vai ser retido e vai ser mandado para a conta do vendedor de forma rápida, prática e segura.

Durante todo esse processo a loja se comunica com a instituição financeira do seu cliente para verificar a veracidade das informações apresentadas, como saldo do cartão está correto para ser feito a retenção do valor e mandar para o lojista. Estando tudo certo o gateway faz a confirmação da compra, e para o consumidor aparece a mensagem de compra confirmada.

A figura 7 ilustra o resumo visual do funcionamento do gateway:

Figura 7: Funcionamento do Gateway.



Fonte: Mercado pago, 2021.

Como mostrado, o Gateway é essencial para que o SET exerça sua função na comunicação entre seus participantes. Suas funcionalidades entregam segurança a todos os envolvidos no comércio, segue abaixo o motivo.

9.3. Funcionalidades do SET

Provê Autenticação:

- **Autenticação do vendedor:** O SET permite que o comprador da mercadoria tenha acesso para visualizar a relação entre o vendedor e o instituto

bancário. Para essa visualização o SET usa o certificado X.509V3 (formato padrão para certificados de chave pública)

- **Autenticação para o comprador:** Checa se o uso do cartão é feito por usuário que está usando o certificado X.509V3.

Provê Confidencialidade e Integridade:

O uso do SET também provê confidencialidade e integridade da mensagem. A confidencialidade não permite que a mensagem enviada seja lida por outro usuário, e para isso é usado o algoritmo de encriptação DES (*Data Encryption Standart*).

A integridade, por sua vez, não permite que a mensagem seja alterada durante o envio com a ajuda das assinaturas digitais. As mensagens são protegidas usando assinatura digital RSA para não ser modificada por usuários não autorizados.

9.4. Dual Signature

O *Dual Signature* consiste em linkar duas informações distintas, porém referentes a mesma compra. Essas informações são: ***Payment Information*** *e* ***Order Information****.*

Payment Information**:** Informações relacionadas ao pagamento, como o número de cartão, validade, nome do proprietário do cartão, entre outros. Essas informações são direcionadas apenas para o banco.

Order Information**:** Informações do pedido, ou seja, do produto comprado, quantidade, garantia, entre outros. Essas informações são direcionadas apenas para o vendedor.

Essas informações são separadas, pois o banco não precisa das informações do pedido, e o vendedor não precisa das informações do cartão do comprador, dessa maneira cada participante do SET acaba recebendo somente as informações necessárias.

Porém, por questões de segurança, essas duas informações ainda precisam estar conectadas de alguma forma, para que o comprador da mercadoria possa provar

que o pagamento efetuado é referente ao pedido feito, e não a algum outro serviço ou produto.

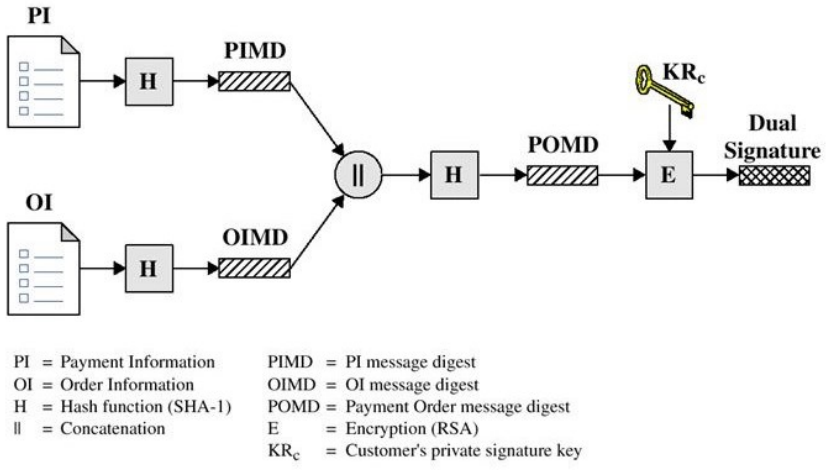
Para isso é necessário aplicar a função criptográfica ***hash*** (utilizando o SHA-1) na *Order Information* e no *Payment Information*.

Segundo Monteiro (2008, p.11), “A função de *hash* gera um resumo, ou seja, uma função de *hash* resume em uma linha de código um documento inteiro”, isso aumenta o desempenho e ganha-se tempo no processo de geração de assinatura digital.

Após isso os dois ***hashes*** são conectados e mais uma vez é usado a função *hash*. O resultado após essa *hash* é finalmente criptografado com a assinatura do comprador, criando então o ***Dual Signature***.

Segue figura 8 que demonstra como funciona o *Dual Signature*:

Figura 8: Funcionamento do *Dual Signature*.



Fonte: Dept. of ISE, 2012

9.5. *Purchase Request* (comprador para vendedor)

O *Purchase Request* (Requisição de compra) consiste na maneira em que as informações da compra serão enviadas do comprador para o vendedor.

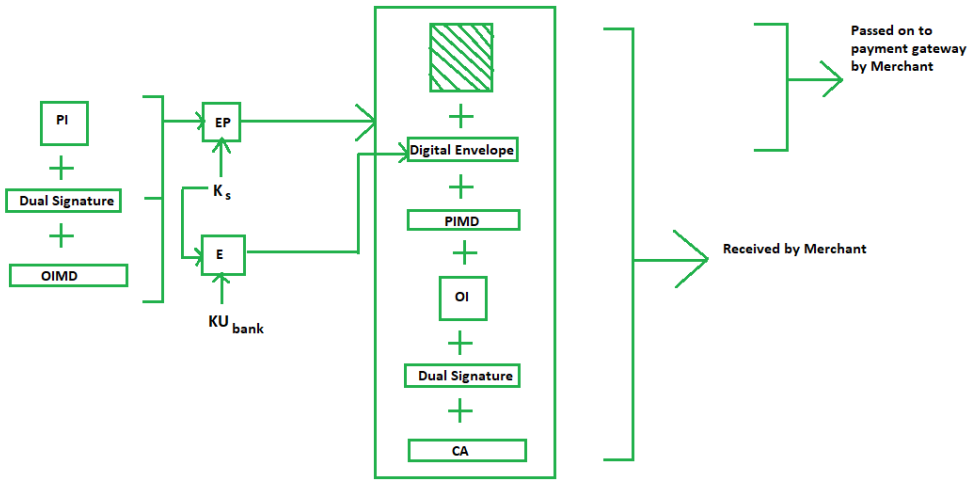
Primeiramente será feita a criptografia do *Payment Information* + OIMD + *Dual Signature*, utilizando a Chave Simétrica Temporária (Ks), que por sua vez também é criptografada com a Chave Pública do Banco (Instituto financeiro). Essa criptografia

do Ks utilizando a Chave Pública do Banco é designado por DS *(Digital Envelop* - Envelope Digital).

Após esse processo, será enviada uma série de informações para o vendedor, sendo elas: mensagem criptografada, envelope digital, PIMD, OI, DS, CA (Certificado do usuário).

Na Figura 9 observa-se a estrutura de envio:

Figura 9: Estrutura do *Purchase Request*.



Fonte: Geeks for Geeks, 2021.

Para desencriptar essa mensagem o vendedor deve saber a Chave Primária Temporária (Ks), a qual está inserida no Envelope Digital, criptografada utilizando a Chave Pública do banco. Portanto, apenas o banco pode decifrar a mensagem e a chave simétrica temporária utilizando sua chave privada, tornando o compartilhamento de informações mais seguro.

9.6. *Payment Autorization* (pelo Banco/Instituto financeiro)

Essa etapa se define pelo processo envio da mensagem e envelope digital criptografados, do vendedor para o banco, que por sua vez irá descriptografar as informações e conferir sua integridade.

Primeiramente o banco irá usar sua chave privada para descriptografar o envelope digital, assim tendo acesso à chave simétrica temporária. Com essa chave

é possível decifrar a mensagem, tendo então o *Payment Information*, OIMD e o *Dual Signature.*

Após isso o banco irá executar o *hash* no *Payment Information* para obter o PIMD, o qual será conectado com o OIMD para ser executado novamente o *hash* e obter finalmente o POMD.

Para saber se o POMD gerado está correto, o banco irá descriptografar o *Dual Signature* utilizando sua chave pública, assim descobrindo o POMD que foi enviado pelo vendedor.

Após isso, o banco irá comparar o POMD gerado com o POMD enviado pelo vendedor a fim de descobrir a integridade da mensagem.

9.7. *Payment capture* (requisitado pelo vendedor para Acquirer)

Após as duas etapas acima forem completas, realiza-se o *Payment Capture*, onde o gateway irá conferir as informações e autorizações da compra e enfim fazer a transação da conta do comprador para a conta do vendedor, completando a compra.

10. Leis Brasileiras aplicadas no E-commerce.

Todos os pontos citados no desenvolvimento do trabalho visam dar o máximo de segurança para todos os envolvidos em uma transação eletrônica, porém, como diz uma famosa frase cujo autor é desconhecido, “nada é cem por cento seguro”.

O objetivo dessa frase e enfatizar o fato que, mesmo um aplicativo, site, servidor, ou qualquer outro meio de informação que possua todo tipo de sistemas de segurança a fim de não ter suas informações roubadas, não é cem por cento seguro.

Todos os tipos de tecnologias podem apresentar erros, todas as empresas estão sujeitas em terem suas informações confidenciais roubadas ou alteradas, independente de toda tecnologia de defesa por trás dessas informações, até mesmo os funcionários, se mal-intencionados ou mal treinados, podem comprometer a segurança da informação.

Segundo Volpini (2021) “hoje, 70% dos golpes feitos no mundo digital estão relacionados a engenharia social”, esse dado mostra a importância de treinar os funcionários a estarem preparados contra esses ataques.

Também por conta desses dados e da possibilidade de pessoas mal-intencionadas estarem inseridos no comércio eletrônico e acabarem roubando informações, ou não cumprindo sua parte do acordo, foram implementadas diversas leis no cenário do *e-commerce* brasileiro.

Veja a seguir as principais leis e seus objetivos com a segurança.

10.1. Lei de proteção de dados (LGPD) (Lei nº 13.709/2018)

A LGPD é uma lei criada em 201 que tem como objetivo determinar como as empresas irão fazer o controle de dados dos brasileiros ou qualquer pessoa localizada no território brasileiro. Ela define o que são dados pessoais e dados pessoais sensíveis e deixa claro que alguns desses dados precisam de mais cuidados.

Os dados pessoais são todo tipo de dados que torna uma pessoa física identificável, ou seja, todos os dados que são diretamente ligados à pessoa física, como RG, CPF, nome, entre outros.

Dados como endereço, placa de carro, profissão, entre outros, apesar de não remeterem diretamente a pessoa física, através de cruzamentos de informações, o

indivíduo pode ser identificado, por conta disso esses dados também podem ser considerados dados pessoais.

Dados pessoais sensíveis são informações que podem levar a fragilidade ou discriminação do titular, tais como origem racial, saúde, vida sexual, convicção religiosa, opinião política, entre outros. A lei LGPD visa proteger todos esses dados.

No artigo 11º deixa claro que é essencial o consentimento do titular dos dados, e que ele pode solicitar que as informações sejam excluídas, transferidas, entre outras ações.

A fiscalização da lei é feita através da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e de outros agentes, os quais são: o controlador, que decide o tratamento das informações; operador, efetua o tratamento; e o encarregado, o qual faz a função de se comunicar com os titulares dos dados pessoais e com a autoridade nacional.

Código de Defesa do Consumidor (Lei n.º 8.078/1990):

O Código de Defesa do Consumidor visa proteger o consumidor e dá outras providências.

É bem verdade que essa lei é antiga, na época em que foi criada, as pessoas ainda não imaginavam o surgimento do comércio eletrônico, portanto os direitos que possuem nessa lei, principalmente no artigo 49, o qual será dado destaque, não podem ser encarados como absoluto, mas ainda são validos e será mais bem explicado a seguir.

No artigo 49 da lei n.º 8.078/1990 é tratado a respeito do direito do arrependimento. De acordo com esse artigo, o consumidor pode desistir do contrato estabelecido dentro do prazo de 7 dias após ter recebido a mercadoria ou serviço.

No momento em que o cliente exercer esse direito, o consumidor deve ser reembolsado de forma imediata.

Porém, como o abuso no comércio eletrônico pode vir por parte do comerciante, ele também pode vir por parte do consumidor. A fim de ganhar vantagem em cima da lei, vários comerciantes exerceram esse direito após terem feito o uso do produto comprado.

Portanto, segundo Vianna (2019):

> “[...] para que o direito de arrependimento seja exercido de forma eficaz, é necessário que, no momento da compra de produtos e/ou serviços, as Políticas de Troca e de Arrependimento do Fornecedor sejam observadas, a fim de evitar eventual litígio.”

Lei do E-Commerce (Decreto Federal n.º 7.962/2013)

Esse decreto determina que as informações da compra devem ser claras e precisas, as características e especificações do produto ou serviço devem ser informadas, até mesmo algum possível risco a saúde que o produto pode trazer.

Essa determinação que regulamenta a lei anterior (lei 8.078/1990) já fica explícito logo no artigo 1º, que possui os seguintes pontos:

I. informações claras a respeito do produto, serviço e do fornecedor;
II. atendimento facilitado ao consumidor; e
III. respeito ao direito de arrependimento

Esse artigo tenta evitar que consumidores adquiram um produto ou serviço sem realmente saber do que se trata por não ter as informações básicas necessárias na página.

Outro ponto para segurança do consumidor no comércio eletrônico está presente no artigo 4º, o qual determina a necessidade de apresentar o sumário do contrato antes da contratação.

Esse sumário deve conter todas as informações da compra para o pleno exercício do direito de escolha do consumidor.

Complementando o artigo 1º, o artigo 5º determina que o fornecedor deve informar de forma clara a maneira eficaz e adequada para o exercício do direito de arrependimento pelo consumidor, ou seja, informar todas as etapas para que o consumidor consiga fazer a devolução do produto, caso ele esteja insatisfeito com a compra ou o produto não atendeu suas necessidades.

Importante destacar a presença do artigo 7º, o qual diz que, caso as determinações feitas nesse decreto não forem cumpridas, será aplicada as sanções previstas no artigo 56 da Lei n.º 8.078, de 1990. Essas sanções podem ser multa, apreensão do produto, proibição de fabricação do produto, entre outros.

11. CONCLUSÃO

A partir das informações apresentadas, pode-se concluir que o comércio eletrônico passou por uma grande evolução, principalmente por conta da pandemia começada em 2020, pois é um método muito prático que permite que os clientes adquiram produtos desejados sem sair de casa.

No dia a dia, com o uso da internet, os usuários estão constantemente expostos a ameaças externas, sendo elas links maliciosos ou pessoas mal-intencionadas cujo objetivo é roubar suas informações, como senhas de cartões, acesso à conta bancárias, número de cartão, entre outros.

Por conta desse aumento no uso do comércio eletrônico no dia a dia das pessoas, também houve um aumento de investimento nessa tecnologia por parte das empresas, isso inclui a segurança das informações, o qual se torna um grande pilar no assunto comércio eletrônico.

Com isso em mente, as empresas passaram a utilizar várias ferramentas para diminuir o risco de furtos em transações eletrônicas. As principais ferramentas utilizadas para alcançar esse objetivo são *firewalls*, SET, criptografia, entre outros, os quais estão detalhadas no desenvolvimento do trabalho.

As formas de trabalho dessas ferramentas garantem que todos os indivíduos envolvidos no negócio se sintam seguros, mostra a importância da segurança da informação no comércio eletrônico, e que sem elas os casos de roubos em transações eletrônicas seriam muito maiores, tornando o mercado muito menor.

REFERÊNCIAS

Albertin, Luiz, Albert et al. **Comércio Eletrônico: Seus Aspectos de Segurança e Privacidade,** 1998. Disponível em: <https://www.scielo.br/j/rae/a/Hyv5cRxyJ7yddLdW6X7xxdc/?format=pdf&lang=pt>. Acesso em 14 out. 2022.

BRASIL. Decreto n.º 7962, de 15 de março de 2013. **Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico**. Diário Oficial da República Federativa do Brasil. Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm>. Acesso em 21 nov. 2022.

BRASIL. Decreto n.º 8078, de 11 de setembro de 1190. **Dispõe sobre a proteção do consumidor e dá outras providências**. Diário Oficial da República Federativa do Brasil. Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm#art5>. Acesso em 21 nov. 2022.

FGV. **A hora e a vez do e-commerce: com pandemia, comércio online mais que dobra e já chega a 21% das vendas do varejo.** Disponível em: <https://cev.fgv.br/noticia/a-hora-e-a-vez-do-e-commerce-com-pandemia-comercio-online-mais-que-dobra-e-ja-chega-a-21-das>. Acesso em 25 set. 2022.

GIANDOMENICO, Diego. **O que é B2C, B2B, B2E, B2G, B2B2C, C2C e D2C + novos modelos de negócio**, 2017. Disponível em: https://olist.com/blog/pt/como-empreender/planejamento-estrategico/o-que-e-b2c-b2b-b2e-b2g-b2b2c-c2c-d2c0/ Acesso em 21 ago. 2017.

GUSMÃO, Amanda. **Entenda o que é B2B, o modelo de negócios business to business**, 2019. Disponível em: https://rockcontent.com/br/blog/b2b/. Acesso em 21 Nov 2022.

KANTHETY, Sundeep Saradhi. **NETWORK SECURITY - SECURE ELECTRONIC TRANSACTION(SET) - PART 1.** Youtube, 31 de mar. de 2018. Disponível em: <https://www.youtube.com/watch?v=Fu82aJJ3tQQ>. Acesso em 5 out. 2022.

KANTHETY, Sundeep Saradhi. **NETWORK SECURITY - SECURE ELECTRONIC TRANSACTION (SET) - PART 2.** Youtube, 31 de mar. de 2018. Disponível em: <https://www.youtube.com/watch?v=BkRLp7rYnc4>. Acesso em 5 out. 2022.

KATTAMURI, Meghna. **Secure Electronic Transaction (SET) Protocol.** Geeks for geeks, 2021. Disponível em: <https://www.geeksforgeeks.org/secure-electronic-transaction-set-protocol/>. Acesso em 12 set. 2022.

KUROSE, James F; ROSS, Keith W. **Rede de computadores e a internet**, uma abordagem *top-down*. 6ª.ed. São Paulo: Pearson Education do Brasil, 2013.

LOPES, Guilherme. **Na pandemia, comércio on-line dobrou número de vendas.** REVISTA OESTE, 17 de out. de 2021. Disponível em: <https://revistaoeste.com/economia/na-pandemia-comercio-online-dobrou-numero-de-vendas/> Acesso em 25 set. 2022.

MAZZOLA, Carolina. **E-commerce: Como Funciona o Comércio Eletrônico?,** 2021. Disponível em: <https://blog.nubank.com.br/e-commerce-como-funciona-o-comercio-eletronico//%3E>. Acesso em 10 out. 2022.

MCAFEE. **O que é um firewall?.** Disponível em: <https://www.mcafee.com/pt-br/antivirus/firewall.html#:~:text=Os%20firewalls%20são%20programas%20de,sua%20conexão%20com%20a%20Internet.> Acesso em 18 out. 2022.

Minuto da Segurança. **Firewall 5 tipos diferentes explicados para você escolher.** 7 de abr. de 2021. Disponível em: <https://minutodaseguranca.blog.br/firewall-5-tipos-diferentes-explicados-para-voce-escolher/>. Acesso em 21 out. 2022.

REIS, Fabio dos. **O que é um Firewall - Segurança de redes.** Youtube, 30 de maio de 2017. Disponível em: <https://www.youtube.com/watch?v=Qg7mhOXH7QY&t=305s>. Acesso em 21 out. 2022.

VIANNA, Carla. **E-COMMERCE: CONHEÇA AS PRINCIPAIS LEIS QUE REGEM A MODALIDADE DE NEGÓCIO**. E-commerce Brasil, 2019. Disponível em: <https://www.ecommercebrasil.com.br/artigos/e-commerce-principais-leis>. Acesso em 21 nov. 2022.