TEXTO-BASE

Segurança dos sistemas de informação e comércio eletrônico

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

Segurança da informação significa proteger seus dados e sistemas de informação de acessos e uso não autorizados, divulgação, modificação, leitura, gravação, inspeção e destruição. Este conceito está relacionado à confidencialidade, integridade e disponibilidade da informação. Já o conceito de segurança de processamento está ligado à disponibilidade e operação da infraestrutura computacional. Esses conceitos são complementares e asseguram a proteção e a disponibilidade das informações das organizações. O impacto da perda de dados, ou até mesmo da violação de informações para uma empresa, é enorme e pode, em alguns casos, levá-la a falência.

Portanto, a segurança em sistemas de informação objetiva a proteção das informações dos clientes e da empresa, a fim de garantir a continuidade do negócio e minimizar os riscos de revelação ou alteração por pessoas não autorizadas. Também está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou para uma organização.

FLUXO DA SEGURANÇA DA INFORMAÇÃO

Ameaça é algo que pode provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio. Essas ameaças podem ser classificadas como:

- *Externas,* representadas por todas as tentativas de ataque e desvio de informações vindas de fora da empresa. Normalmente, essas tentativas são realizadas por pessoas com a intenção de prejudicar a empresa, ou utilizar seus recursos para invadir outras empresas.
- *Internas*, que estão presentes, independentemente de as empresas estarem ou não conectadas à internet. Podem causar desde incidentes leves até os mais graves, como a inatividade das operações da empresa.

Como tipos de ameaças, podemos citar funcionários descontentes, criminosos, terroristas, concorrentes, natureza, imprensa etc.

O grande desafio é proteger os ativos digitais, os dados e, principalmente, o conhecimento.

Podemos entender por ativos digitais tudo aquilo que engloba conteúdos e estratégias usados por uma empresa para atrair clientes, consolidar sua marca e divulgar seus produtos e serviços, independente do meio, mas desde que esteja na rede de computadores, disponível ou não na internet.

Essas ameaças, mediante a exploração de uma determinada vulnerabilidade – que pode ser um erro de software, controles ineficientes, processos interrompidos, falhas no hardware, mudanças nos negócios e, principalmente, erro humano –, elevam os riscos das tecnologias da informação na organização e potencializam as ameaças aos ativos digitais.

Consequentemente, esses ativos necessitam de segurança, mesmo sendo intangíveis, porém de grande valor para as organizações que as detêm.

A forma ideal de as empresas organizarem sua segurança digital é criando políticas de segurança de informação, gerando assim medidas de controle que possam reduzir essas ameaças. Mas é bom ressaltar que esse é um fluxo contínuo e permanente, uma vez que sempre surgem novas ameaças e pontos de vulnerabilidades nas empresas.

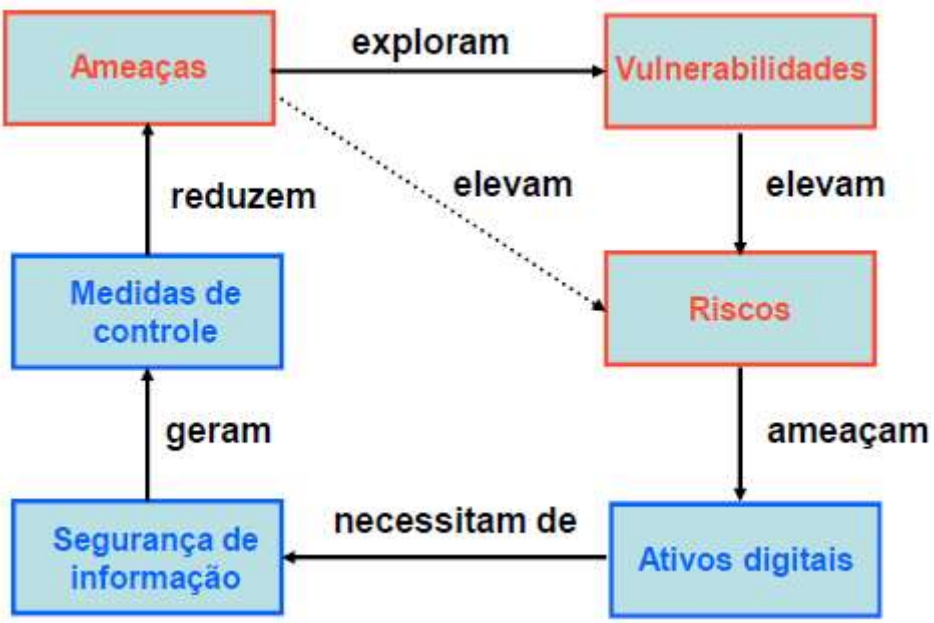

Figura 1 – Fluxo de segurança da informação

Tipos de ativos

Ativos são os elementos que sustentam a operação do negócio. Eles podem ser classificados de diversas formas dependendo do contexto em que estejam sendo abordados, portanto vamos agrupá-los nas formas mais comuns:

- *Tangíveis* – informações impressas, móveis, hardware (como impressoras, scanners);
- *Intangíveis* – marca de um produto, nome da empresa, confiabilidade de um órgão federal;
- *Lógicos* – dados ou informações armazenadas em uma rede, sistema de gestão integrada (ERP);
- *Físicos* – galpão, sistema de eletricidade, estação de trabalho etc.;
- *Humanos* – funcionários, terceirizados etc.

CONTEXTO DA SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

Como é sabido, um dos bens mais importantes para as empresas é a informação. Ela é o motor que faz com que a companhia cresça e pode ser também o principal meio pelo qual uma empresa ganha dinheiro. Sendo assim, os cibercriminosos buscam comprometer a informação das empresas por meio de ataques, invasões em massa, até campanhas de invasões agrupadas que se estabelecem a cada semana.

Com o objetivo de proteger os dados corporativos de clientes, fornecedores de software de segurança e até cidadãos, as empresas implementam cada vez mais medidas de segurança para assegurar a informação. Obviamente, não é algo fácil de se realizar, e muitas vezes o principal problema é que é difícil de saber por onde começar: relevar as políticas de segurança, classificar a informação, educar os usuários, adquirir tecnologias, e essas são apenas algumas das ações.

Um bom ponto de partida seria se basear em alguma norma ou ainda alguma lei de proteção de dados pessoais. Quase todos os países da América Latina possuem alguma lei de proteção de dados, ou ainda, estão trabalhando para implementar uma. De modo geral, todas essas leis possuem os mesmos princípios e se baseiam em três aspectos fundamentais: garantir a confidencialidade, integridade e disponibilidade dos dados armazenados. Dependendo do país, o que pode mudar é a penalidade que será aplicada caso haja algum incidente ou descumprimento em relação aos requisitos da lei. Essas penalidades podem ser desde multas financeiras até condenações de prisão por parte do responsável da segurança dos dados, passando pela revogação de permissões para exercer alguma atividade específica.

A tríade CIA (*confidentiality, integrity and availability*) – confidencialidade, integridade e disponibilidade – representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são não repúdio (irretratabilidade), autenticidade e conformidade. Com

a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

Confidencialidade

Refere-se a proteger informações de serem acessadas por pessoas não autorizadas. Em outras palavras, apenas pessoas autorizadas a fazer isso podem ter acesso a dados confidenciais. Imagine seus registros bancários. Você deve acessá-los, é claro, e pessoas que trabalham no banco e estão ajudando com as transações também, mais ninguém. Uma falha em manter a confidencialidade significa que alguém que não deveria ter acesso consegue obtê-lo intencionalmente ou por acidente. Tal falha de confidencialidade, também conhecida como *breach*, normalmente não pode ser recuperada. Uma vez que o segredo tenha sido revelado, não há como esconder. Se seus registros bancários forem publicados em site, todos poderão saber o número da sua conta bancária, o saldo etc., e essas informações não poderão ser apagadas de suas mentes, documentos, computadores e outros locais. Quase todos os principais incidentes de segurança relatados na mídia hoje envolvem grandes perdas de confidencialidade.

Integridade

Refere-se a garantir a autenticidade da informação: essa informação não é alterada e a fonte dela é segura. Imagine que você tem um site em que vende produtos. Agora imagine que um invasor pode fazer compras em seu site e alterar os preços dos produtos de maneira mal-intencionada, para que possa comprar qualquer coisa pelo preço que escolher. Essa seria uma falha de integridade, porque sua informação – nesse caso, o preço de um produto – foi alterada sem sua autorização. Outro exemplo de falha de integridade é quando você tenta se conectar a um site, e um invasor mal-intencionado entre você e o site redireciona o tráfego para um site diferente. Nesse caso, o site para o qual você é direcionado não é genuíno.

Disponibilidade

Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

POLÍTICA DE SEGURANÇA

O estabelecimento de uma política de segurança da informação em sua empresa deve passar sempre por ações que norteiem esses princípios. Tal modelo deve estar amparado por um sistema de gestão de segurança da informação que precisa ser planejado e organizado, implementado, mantido e monitorado. Muitas organizações não seguem essa abordagem no desenvolvimento, implementação e manutenção de seu programa de gestão de segurança. Isso porque talvez não conheçam ou entendam que essa abordagem é de difícil implementação ou uma perda de tempo.

Uma política de segurança da informação tem por objetivo possibilitar o gerenciamento da segurança em uma organização, estabelecendo regras e padrões para proteção da informação. A política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário. Os controles devem ser definidos levando em conta as características de cada empresa, definindo o que é permitido e o que é proibido. A implantação, para ser bem-sucedida, deve partir da diretoria da empresa para os demais funcionários (abordagem *top down*). A política deve ser divulgada para todos os funcionários da organização, de forma a manter a segurança das informações.

As políticas de segurança devem ter implementação realista e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se às alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Existem duas filosofias por trás de qualquer política de segurança:

- A *proibitiva* (tudo o que não é expressamente permitido é proibido);
- A *permissiva* (tudo o que não é proibido é permitido).

Os elementos *disponibilidade, integridade* e *confidencialidade*, citados no contexto da política de segurança da informação, devem ser considerados. Além desses, também podemos citar:

- A *autenticidade*, isto é, o sistema deve ter condições de garantir de que a informação e/ou a identidade dos usuários são o que dizem ser;
- A *legalidade*, isto é, o valor legal das informações dentro de um processo de comunicação.

Portanto, uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

ACORDO DE NÃO DIVULGAÇÃO

Um acordo de não divulgação (*non-disclosure agreement* – NDA –, ou também conhecido como *confidential disclosure agreement* – CDA), um termo de confidencialidade ou acordo secreto, é um contrato legal entre ao menos duas partes que destacam materiais ou conhecimentos confidenciais que essas partes desejam compartilhar para determinado propósito, mas cujo uso generalizado desejam restringir.

É um contrato através do qual as partes concordam em não divulgar informação coberta pelo acordo. Um acordo de não divulgação cria um relacionamento confidencial entre as partes para proteger qualquer tipo de segredo comercial.

MECANISMOS DE SEGURANÇA

Há diversos mecanismos de segurança de dados e informação. As recomendações de segurança podem ser encontradas nas seguintes formas:

Controles físicos

São barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura (que garante a existência da informação) que a suporta. Mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem, guardas etc.

Controles lógicos

São barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta à

alteração não autorizada por elemento mal-intencionado. Mecanismos de segurança que apoiam os controles lógicos podem ser encontrados a seguir:

- *Mecanismos de cifração ou encriptação* – permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se, para tal, de algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

Figura 2 – Processo de criptografia dos dados enviados do emissor ao receptor.

- *Assinatura digital* – um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade.

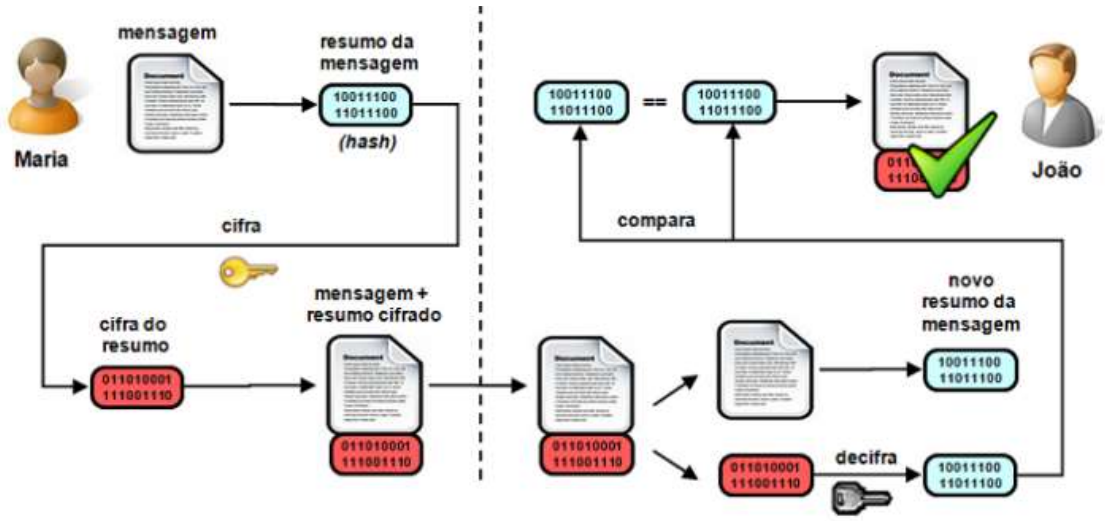

Figura 3 – Processo de assinatura digital

- *Mecanismos de garantia da integridade da informação* – usando funções de *hashing*, como citado anteriormente, ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.

- *Mecanismos de controle de acesso* – palavras-chave, sistemas biométricos, firewalls, cartões inteligentes etc.

- *Mecanismos de certificação* – atestam a validade de um documento. Podem ser vistas como um conjunto de técnicas, processos e normas estabelecidas ou adotadas que visam propiciar mais segurança às comunicações e transações eletrônicas, proporcionando a autenticidade e integridade das informações que tramitam de forma eletrônica. Logo, pode-se dizer que ela é necessária ou recomendada sempre que se deseje aumentar o nível de segurança nos serviços de autenticação de usuários, servidores, aplicações, pois garante as propriedades de confidencialidade, autenticidade, integridade e não repúdio.

Figura 4 – Tipos físicos de certificados digitais A3 (cartão) e A1 (pen-drive)

- *Honeypot* – é uma ferramenta que tem a função de, propositalmente, simular falhas de segurança de um sistema e colher informações sobre o invasor enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema. É uma espécie de armadilha para invasores. O *honeypot* não oferece nenhum tipo de proteção específica.

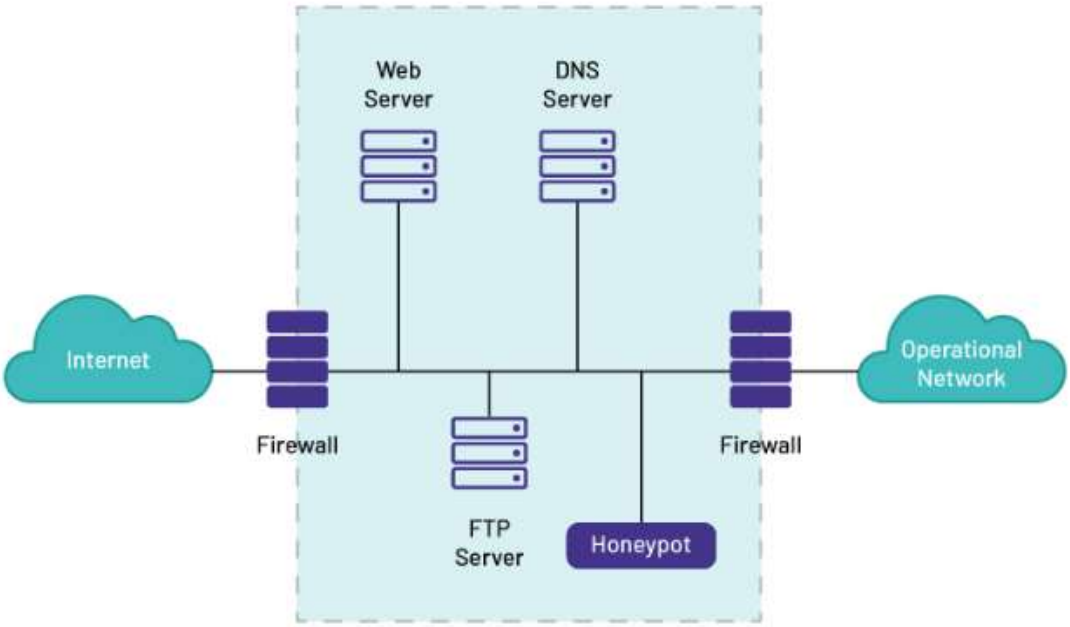

Figura 5 – Arquitetura do *honeypot*

Existe uma grande variedade de ferramentas e sistemas que pretendem fornecer segurança além dos citados anteriormente. Alguns exemplos: antivírus, firewalls, filtros anti-spam, fuzzers (técnica de testes de software), detectores de intrusões, analisadores de código etc.

GESTÃO DE RISCO

A gestão de riscos, por sua vez, fundamental para garantir o perfeito funcionamento de toda a estrutura tecnológica da empresa, engloba a segurança da informação, já que a quantidade de vulnerabilidades e riscos que podem comprometer as informações da empresa é cada vez maior. Ao englobar a gestão da segurança da informação, a gestão de riscos tem como principais desafios:

- *Proteger* um dos principais ativos da organização – a informação – assim como a reputação e a marca da empresa;
- *Implementar* e *gerir* controles que tenham como foco principal os objetivos do negócio;
- *Promover* ações corretivas e preventivas de forma eficiente;
- *Garantir* o cumprimento de regulamentações;
- *Definir* os processos de gestão da segurança da informação.

Entre as vantagens de investir na gestão de riscos voltada para a segurança da informação, estão a priorização das ações de acordo com a necessidade e os objetivos da empresa e a utilização de métricas e indicadores de resultados.

NORMAS DE SEGURANÇA DE INFORMAÇÃO

ISO/IEC 27001 é a norma que define os requisitos para um sistema de gestão da segurança da informação (SGSI). 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. Inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos. A publicação é muito conhecida entre estudantes de concursos de tecnologia de informação.

A ISO 27001 é a principal norma de segurança de tecnologia de informação 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 SGSI. Já a ISO/IEC 27002 é um código de práticas, com um conjunto completo de controles que auxiliam a aplicação do SGSI.

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 de boas práticas.

E-BUSINESS

e-Business, acrônimo do inglês *electronic business* (negócio eletrônico), é o termo que se utiliza para identificar os negócios efetuados por meios eletrônicos, geralmente na internet. São negócios feitos através da internet ou intranet no sentido mais amplo da palavra negócio, desde contatos diretos com consumidores e fornecedores, como também análises de mercado, análises de investimentos, busca de informações sobre o macroambiente, pesquisa de mercados etc.

Baseia-se em um conjunto de sistemas de uma empresa que se interligam e interagem com os sistemas de diversas outras empresas, servindo como a infraestrutura do e-Commerce (comércio eletrônico). Portanto, e-Business tem como aplicação a criação de sistemas capazes de prover comunicação entre empresas, agilizando os processos de compra e venda entre estas. Existem, inclusive, sistemas que fazem pedido automáticos para outras empresas de acordo com o seu

estoque de produtos, facilitando assim todo o processo de fabricação e venda, melhorando a disponibilidade de produtos de acordo com a demanda por estes.

COMÉRCIO ELETRÔNICO

O comércio eletrônico precisa ser evidenciado como uma nova forma de percepção e interação entre a empresa e seus clientes, que agora serão virtuais. O quadro que evoluiu para essa modalidade de comércio foi marcado por procedimentos impostos ao mercado na década de 1980, juntamente com as inovações expostas até aqui em nossos estudos. Esses procedimentos envolviam o desenvolvimento de formas virtuais ou não presenciais de interação com o consumidor, como centrais de telemarketing, catálogos e contatos virtuais em substituição ao contato físico com o produto e, às vezes, até com o vendedor.

Esse modelo de negócio será tratado com mais detalhes nos próximos tópicos.

e-Commerce

O e-Commerce, ou comércio eletrônico, compreende qualquer tipo de transação comercial (com ou sem fins lucrativos) feita especialmente através de um equipamento eletrônico de informática, como computadores, tablets e smartphones, utilizando a internet. Seus fundamentos estão baseados em tecnologia da informação, como aplicativos, segurança, criptografia, moedas e pagamentos eletrônicos. Ele ainda envolve pesquisa, desenvolvimento, marketing, propaganda, negociação, vendas, logística e suporte.

Quando se parte para esse modelo de negócio, várias dúvidas surgem relativas à logística, ao armazenamento e principalmente ao pagamento. Tudo isso vai depender do modo de funcionalidade da empresa e, no caso específico do pagamento, dependerá das opções oferecidas de financiamento para cada serviço de pagamento *on-line*, as conexões (*gateways*), e somente assim decidir qual é mais compatível com sua estratégia de negócio.

Outro fator a se atentar são as métricas e indicadores do e-Commerce, pois assim poderemos analisar o potencial do negócio. Alguns dos indicadores sugeridos são:

- Quantidade de visitantes únicos;
- Taxa de conversão de vendas;
- Taxa de conversão de *upselling* e *cross-selling*;

- Retorno do investimento;
- *Ticket* médio;
- Taxa de abandono de carrinho;
- Taxa de rejeição;
- Custo de aquisição de cliente;
- Taxa de trocas e devoluções;
- Taxa de amplificação.

De qualquer forma, adaptar seu negócio ao e-Commerce, ou até mesmo começar um novo, exige esforço e desafios como os seguintes:

- Integração e colaboração de orientação;
- Funcionalidade;
- Escalabilidade/disponibilidade;
- Segurança;
- Privacidade;
- Conteúdo/catálogo de gestão;
- Arquitetura *hub-and-spoke*.

Portanto, é importante considerar esses elementos para que o egresso nesse modelo de negócio não se torne uma frustação e, principalmente, um grande prejuízo.

Figura 6 – Processo de funcionamento do e-Commerce

e-Marketplace

Começou como sites públicos e privados que agrupavam clientes e fornecedores em um mesmo ambiente virtual, facilitando a negociação em tempo real. Como exemplos, temos Portal Mão na Roda (www.portalmaonaroda.com.br) e Mercado (www.me.com.br). Atualmente, é um espaço virtual em que se faz comércio eletrônico no sentido mais amplo. Trata-se de vender seus produtos, dentro dos grandes e-Commerces, como Submarino, Ponto Frio, Mercado Livre, Casas Bahia, entre outros. O produto de sua loja virtual vai aparecer dentro dos grandes e-Commerces, será vendido por eles e entregue por você.

Utilizando e-Marketplace, você elimina diversas tarefas que sua empresa precisa realizar, como SAC, publicidade, taxas com cartões, *chargebacks* (cancelamento de uma venda feita com cartão de débito ou crédito) etc., gerando, portanto, economia. Colocar seu produto dentro de sites com milhões de visitas por dia, resulta em vendas e gera lucros, aumentando seus resultados.

e-Procurement

Sites que realizam a cotação on-line de produtos com vários fornecedores, fechando a transação com a ajuda de um sistema de gestão de recursos empresariais (ERP). Por exemplo, Mercado Eletrônico (www.me.com.br) e Já Cotei (www.jacotei.com.br). O e-Procurement possibilita um fator fundamental no mundo dos negócios, agiliza os processos internos e dispõe produtos mais rapidamente no mercado através da internet. O e-Procurement pode se tornar uma vantagem competitiva quando bem estruturado e alinhado estrategicamente com os principais parceiros de negócio da organização.

Modelos de e-Commerce

Quando falamos em tipos de e-Commerce estamos nos referindo às diversas configurações possíveis em uma atividade de venda pela internet. Uma atividade comercial pela internet pode ser estruturada com base em diversos modelos de negócios no e-Commerce, em função principalmente do tipo de relação entre as partes compradora e vendedora.

É importante conhecer detalhes sobre os modelos de e-Commerce para que se possa estruturar o seu planejamento em função das características próprias de cada

um desses modelos. Existem diversos modelos, mas escolheremos os principais e mais comuns:

- B2B (*business to business*) – no caso do público, são vários fornecedores que disponibilizam seus produtos para venda a outras empresas em determinado segmento de mercado; no caso do privado ou particular, um único fornecedor vende seus produtos para seus representantes, revendedores e lojistas.
- B2C (*business to consumer*) – é uma forma de comércio eletrônico na qual os clientes tratam diretamente com uma empresa para evitar intermediários. Os pioneiros do B2C competiam com os tradicionais varejistas em um ramo de negócios e vendiam seus produtos diretamente aos clientes.
- C2C (*consumer to consumer*) – um subconjunto de comércio eletrônico que envolve transações eletrônicas entre clientes por meio de um terceiro que facilita o processo. O eBay é um exemplo: os clientes compram e vendem itens entre si pelo site. Fundado em 1995, tem se tornado um dos sites mais populares do mundo.
- B2G (*business to governement*) – as negociações entre empresas e governo são chamadas de B2G. Geralmente, esse tipo de relação passa por um processo de licitação (concorrência pública), como é o caso de montadoras de veículos que desejam fornecer frota de carros para a polícia, ou ainda empreiteiras que visam a construção de obras públicas (rodovias, escolas etc.).

FUTURO DO E-COMMERCE

Com a evolução da tecnologia de informação, muitos serviços têm evoluído e novas formas de se fazer negócio tem surgido. Vamos citar algumas que despontam como as mais promissoras:

M-Commerce / mobile commerce

O *mobile commerce* ou m-Commerce é toda a transação comercial de bens e serviços feita através de dispositivos móveis. Para realizar a compra, o consumidor utiliza aparelhos como smartphones e tablets, e suas funcionalidades, como aplicativos de acesso às lojas virtuais. Considerado uma evolução do e-Commerce, essa nova modalidade de comércio eletrônico é uma oportunidade de conquistar clientes que vivem conectados e que realizam cada dia mais compras pelos dispositivos móveis.

O m-Commerce também se aproveita da interatividade com as redes sociais para potencializar as vendas. Através dessa tecnologia, é possível compartilhar suas experiências de compra virtual com seus amigos, o que amplia a influência da marca e aumenta as chances de novas vendas.

T-Commerce / television commerce

O t-Commerce permite realizar compras enquanto se assiste à programação do canal aberto. Trata-se de um modelo de negócio que une tecnologia e conteúdos pouco explorados, que integra dois segmentos em franca expansão: TV somada a seus serviços de *streaming* e plataformas e o tradicional e-Commerce, que resultam na união do entretenimento com o mundo do comércio eletrônico. Com o passar dos anos, em uma velocidade cada vez maior, outras áreas da tecnologia se juntarão ao t-Commerce. Isso acontecerá porque hoje temos uma demanda de consumidores ávidos por novas experiências e facilidades que permitam a eles fazer parte desse novo mundo, não só com acesso rápido e de qualidade aos seus conteúdos favoritos, mas também a novas oportunidades de maximizar sua experiência multiplataforma com cada vez menos interrupções.

Marketing digital

Atrelado a toda essa movimentação, surge com força o marketing digital, que consiste em ações de comunicação que as empresas podem utilizar por meio da internet, da telefonia celular e de outros meios digitais, para assim divulgar e comercializar seus produtos, conquistando novos clientes e melhorando sua rede de relacionamentos. Ele engloba a prática de promover produtos ou serviços pela utilização de canais de distribuição eletrônicos, para então chegar aos consumidores rapidamente de forma relevante, personalizada e com mais eficiência.

LEGISLAÇÃO DO COMÉRCIO ELETRÔNICO

A legislação do e-Commerce é composta, principalmente, de dois materiais: o Código de Defesa do Consumidor (CDC), criado em 1990, quando o comércio eletrônico praticamente não existia, portanto sem elementos específicos para o comércio pela internet, e o decreto nº 7.962/2013, que completou as lacunas e passou a vigorar em paralelo ao CDC, tornando-se o principal regulamento do e-Commerce no Brasil.

Algumas das obrigações e regras que foram detalhadas nesse decreto:

- Exigência de identificação completa do fornecedor no site;
- Exigência do endereço físico e eletrônico no site;
- Informações devem ser claras e precisas.

Outros pontos que são tratados pelo decreto:

- Informação para os consumidores das condições da compra;
- Facilitação para o atendimento das demandas do cliente;
- Canais de atendimento;
- Facilitação da devolução dos produtos no caso de arrependimento, entre outras coisas.

Referências bibliográficas

1. AUDY, Jorge L.N.; ANDRADE, Gilberto K.; CIDRAL, Alexandre. **Fundamentos de sistemas de informação**. Porto Alegre: Bookman, 2007. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788577801305/cfi/0!/4/2@100:0.00>. Acesso em: 26 mar. 2019.
2. BATISTA, Emerson de Oliveira. **Sistemas de informação**: o uso consciente da tecnologia para o gerenciamento. 2. ed. São Paulo: Saraiva, 2012. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502197565/cfi/0>. Acesso em: 26 mar. 2019.
3. **Decreto nº 7.962, de 15 de março de 2013**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm >. Acesso em: 26 mar. 2019.
4. CAIÇARA JR., Cícero. **Sistemas integrados de gestão ERP**: uma abordagem gerencial. 2. ed. Curitiba: InterSaberes, 2015. Disponível em: <http://univesp.bv3.digitalpages.com.br/users/publications/9788544301616/pages/-2>. Acesso em: 26 mar. 2019.
5. CRUZ, Tadeu. **Manual de técnicas administrativas**: métodos e procedimentos com formulários. São Paulo: Atlas, 2018. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597018653/cfi/6/2!/4/2@0:0>. Acesso em: 26 mar. 2019.
6. FUNDAÇÃO PROCON. **Código de proteção e defesa do consumidor**: lei nº 8.078, de 11 de setembro de 1990. São Paulo: PROCON, 2018. Disponível em: <http://www.procon.sp.gov.br/pdf/CDCcompleto.pdf >. Acesso em: 26 mar. 2019.

7. HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. Disponível em: <https://univesp.bv3.digitalpages.com.br/users/publications/9788574528670>. Acesso em: 26 mar. 2019.
8. JOÃO, Belmiro N. (Org.). **Sistemas de informação**. São Paulo: Pearson Education do Brasil, 2012. Disponível em: <http://univesp.bv3.digitalpages.com.br/users/publications/9788564574533/pages/-12>. Acesso em: 26 mar. 2019.
9. JOÃO, Belmiro N. (Org.). **Tecnologia da informação gerencial**. São Paulo: Pearson Education do Brasil, 2015. Disponível em: <http://univesp.bv3.digitalpages.com.br/users/publications/9788543014746/pages/-14>. Acesso em: 26 mar. 2019.
10. LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informação gerenciais**. 11. ed. São Paulo: Pearson Education do Brasil, 2014. Disponível em: <http://univesp.bv3.digitalpages.com.br/users/publications/9788543005850/pages/-22>. Acesso em: 26 mar. 2019.
11. LIMA-CARDOSO, André; SALVADOR, Daniel O.; SIMONIADES, Roberto. **Planejamento de marketing digital**: como posicionar sua empresa em mídias sociais, blogs, aplicativos móveis e sites. Rio de Janeiro: Brasport, 2015. Disponível em: <https://univesp.bv3.digitalpages.com.br/users/publications/9788574528281>. Acesso em: 26 mar. 2019.
12. MARINHO, Antonio Lopes (Org.). **Análise e modelagem de sistemas**. São Paulo: Pearson Education do Brasil, 2016. Disponível em: <http://univesp.bv3.digitalpages.com.br/users/publications/9788543017341/pages/-14>. Acesso em: 26 mar. 2019.
13. RABECHINI JR, Roque; CARVALHO, Marly M. (Org.). **Gerenciamento de projetos na prática**: casos brasileiros. São Paulo: Atlas, 2013. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522466702/cfi/0!/4/2@100:0.00>. Acesso em 26 mar. 2019.
14. ROSINI, Alessandro M.; PALMISANO, Angelo. **Administração de sistemas de informação e a gestão do conhecimento**. 2. ed. São Paulo: Cengage Learning, 2012. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522114672/cfi/0!/4/2@100:0.00>. Acesso em: 26 mar. 2019.
15. **Aspectos legais do e-Commerce**. Brasília: SEBRAE, 2014. Disponível em: <https://bibliotecas.sebrae.com.br/chronus/ARQUIVOS_CHRONUS/bds/bds

.nsf/1fb2b554ec81cb7a7da2eeab6ecef4c3/$File/5051.pdf>. Acesso em: 26 mar. 2019.

16. STAIR, Ralph M.; REYNOLDS, George W. **Princípios de sistemas de informação**. 3. ed. São Paulo: Cengage Learning, 2015. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522124107/cfi/0!/4/2@100:0.00>. Acesso em: 26 mar. 2019.