ETEC DR. RENATO CORDEIRO

HABILITAÇÃO PROFISSIONAL TÉCNICA DE NÍVEL MÉDIO
TÉCNICO EM ADMINISTRAÇÃO

Ítalo Gustavo Martins Ratão

Julia Barbato Cruzato

Kaio Marques Mendonça

Mariana Andrade Campos

Tales Santana Borges

Yngrid de Melo Moreira

SEGURANÇA DA INFORMAÇÃO: AMBIENTE CORPORATIVO

BIRIGUI

2024

Ítalo Gustavo Martins Ratão
Julia Barbato Cruzato
Kaio Marques Mendonça
Mariana Andrade Campos
Tales Santana Borges
Yngrid de Melo Moreira

SEGURANÇA DA INFORMAÇÃO: AMBIENTE CORPORATIVO

Trabalho de Conclusão de Curso apresentado à Banca Examinadora da ETEC Doutor Renato Cordeiro de Birigui – SP. Habilitação Profissional Técnica de Nível Médio e Técnico em Administração, sob a orientação do Prof. Anderson Henrique Teixeira de Souza, como requisito para obtenção do título de Técnico em Administração.

BIRIGUI
2024

FOLHA DE APROVAÇÃO

Ítalo Gustavo Martins Ratão

Julia Barbato Cruzato

Kaio Marques Mendonça

Mariana Andrade Campos

Tales Santana Borges

Vinícius Novais Pavanelli

Relatório final, apresentado a ETEC Dr. Renato Cordeiro, como parte da formação para a obtenção do título de Técnico em Administração.

Birigui, 02 de dezembro de 2024.

BANCA EXAMINADORA

_____

Prof. Anderson Henrique Teixeira de Souza

Orientador

_____

Prof. Jessé Tobias da Silva Júnior

Avaliador

_____

Prof. ª Ana Gabriela Arantes Gomes Carvalho

Avaliador

Dedicamos este trabalho a Deus, aos nossos familiares, professores e amigos.

Agradecemos ao nosso professor e orientador Anderson Henrique Teixeira de Souza, aos nossos amigos e todos os envolvidos no desenvolvimento deste trabalho.

"Se quiseres acordar toda a humanidade, então acorda-te a ti mesmo, se quiseres eliminar o sofrimento no mundo, então elimina a escuridão e negativismo em ti próprio. Na verdade, a maior dádiva que podes dar ao mundo é aquela da tua própria auto-transformação." (Lao Tzu 571 a.C.- 517 a.C.)

RESUMO

O presente trabalho aborda a relevância da ética no contexto da segurança da informação, considerando os desafios impostos pela valorização dos dados no ambiente corporativo e tecnológico atual. Evidencia-se a responsabilidade das organizações em garantir a integridade e privacidade das informações pessoais, através da adoção de práticas éticas e transparentes, como a comunicação objetiva sobre a coleta e o uso dos dados e o compromisso com padrões elevados de segurança. O texto critica a prevalência de softwares proprietários, muitas vezes associados a falhas de segurança e ao uso inadequado de dados pessoais, destacando a superioridade de alternativas de código aberto, como sistemas baseados em Unix, Linux e BSD, reconhecidos por segurança e configurabilidade. Ademais, o estudo problematiza as práticas de grandes corporações na exploração de dados de usuários para fins comerciais, reforçando a necessidade de regulamentações mais efetivas, como o aprimoramento da Lei Geral de Proteção de Dados (LGPD), e de um posicionamento político assertivo para coibir abusos. Por fim, enfatiza-se a importância da conscientização dos usuários acerca de seus direitos e da busca por tecnologias que promovam autonomia e segurança, em contraposição à mercantilização de suas informações no cenário global. Destaca também a resposta do serviço comunitário a partir da organização informacional, onde a comunidade, a partir de sua organização, deve trabalhar para si, em benefício de seus constituintes.

Palavras-chave: Segurança da Informação, Lei Geral de Proteção de Dados, Dados Pessoais, Organização Informacional.

ABSTRACT

This paper addresses the importance of ethics in the context of information security, considering the challenges posed by the growing value of data in today's corporate and technological environment. It highlights organizations' responsibility to ensure the integrity and privacy of personal information through the adoption of ethical and transparent practices, such as clear communication about data collection and usage, as well as a commitment to high security standards. The text critiques the prevalence of proprietary software, often associated with security flaws and improper use of personal data, emphasizing the superiority of open-source alternatives, such as Unix, Linux, and BSD-based systems, renowned for their security and configurability.Furthermore, the study examines the practices of large corporations exploiting user data for commercial purposes, underscoring the need for more effective regulations, such as the enhancement of the General Data Protection Law (LGPD), and a more assertive political stance to curb abuses. Finally, it emphasizes the importance of raising user awareness about their rights and encouraging the adoption of technologies that promote autonomy and security, as opposed to the commodification of personal information in the global scenario. The text also highlights the role of community-driven initiatives, stressing that organized communities should work collectively for the benefit of their members.

Keywords: Information Security, General Data Protection Law, Personal Data, Information Organization.

SUMÁRIO

INTRODUÇÃO

Segundo Snowden (2019) a causa do problema da segurança de dados, não é a proteção dos dados, mas sim, a coleta de dados e seu uso indevido. Snowden refere-se à RGPD (Regulamento Geral sobre a Proteção de Dados), com enfoque da situação na União Europeia, como um “Um tigre de papel”, a passo que, esta regula a proteção dos dados, mas não diz respeito à coleta de dados, então, por mais que, medidas sejam impostas a utilização destes dados, como políticas de privacidade e termos de uso, ainda sim, o uso de dados e seus processos, acabam por atender ao interesse do capital privado, em suma, o lucro para com a obtenção de dados e informações.

No Brasil, a lei regente é a LGPD (Lei Geral de Proteção de dados), ou, lei federal nº 13.709 (2018), que prevê:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Inicialmente, aparenta estruturação e qualidade ao cidadão, porém, em suas menores cláusulas demonstra o perigo evidenciado por Snowden, onde, na lei federal nº 13.709 (2018), artigo 7º, é previsto:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> [...]
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> [...]

Ou seja, permite ainda a coleta de dados, por parte das empresas, quando há o consentir por parte do usuário, o que, em primeira mão, não é um problema, porém, a gestão desses dados, sua coleta e venda seguem em um pequeno escape perante a lei, visto que, não há devido monitoramento da circulação desses dados.

No ambiente corporativo, é recorrente o uso de softwares, e serviços externos aos da empresa. Estes, não estão isentos da coleta de dados, assim, uma empresa é obrigada a confiar seus dados a uma empresa externa, sem monitoramento, reféns do consentimento sobre o uso de dados, já que, é necessário o uso destes softwares para suas atividades. Exemplo disso, é a Microsoft, que fornece o sistema operacional Windows para uso geral e gratuito, porém, coleta dados do usuário, e tem tendências a encurralar este, com o uso de navegadores e softwares derivados de seu sistema operacional. No contrato de serviços da Microsoft (2023), é evidenciado:

> Seu conteúdo. Muitos dos nossos Serviços permitem que você crie, armazene ou compartilhe Seu conteúdo ou receba material de outras pessoas. Nós não requereremos judicial ou extrajudicialmente a propriedade do Seu Conteúdo. Seu conteúdo permanece seu, e você é responsável por ele.
>
> [...] Você declara e garante que, durante a vigência destes Termos, você tem (e terá) todos os direitos necessários para que Seu Conteúdo seja carregado, armazenado ou compartilhado nos Serviços ou por meio deles, e que a coleta, o uso e a retenção do Seu Conteúdo não violará nenhuma lei

> ou direito de outras pessoas. A Microsoft não possui, controla, verifica, paga por, endossa ou de outra forma assume nenhuma responsabilidade em relação ao Seu Conteúdo e não pode ser responsável por Seu Conteúdo nem pelo material que outras pessoas carregam, armazenam ou compartilham usando os Serviços;
>
> [...] você concede à Microsoft uma licença de propriedade intelectual mundial e sem royalties para usar Seu Conteúdo, por exemplo, para fazer cópias de, reter, transmitir, reformatar, exibir e distribuir, por meio de ferramentas de comunicação, Seu Conteúdo nos Serviços. Se você publicar seu conteúdo em áreas do Serviço nas quais ele está disponível amplamente online sem restrições, seu conteúdo poderá ser exibido nas demonstrações ou nos materiais que promovem o serviço. Alguns dos Serviços são apoiados pela publicidade. [...] Nossas políticas de publicidade são cobertas em detalhes na Política de Privacidade.

Então, torna-se perceptível o viés de comercialização da informação proveniente da coleta de dados, demonstrado no trecho “[...] Se você publicar seu conteúdo em áreas do Serviço nas quais ele está disponível amplamente online sem restrições, seu conteúdo poderá ser exibido nas demonstrações ou nos materiais que promovem o serviço. Alguns dos Serviços são apoiados pela publicidade.[...]” - ou seja, os termos de armazenagem, coleta e compartilhamento, confirmam o interesse comercial da venda da informação.

Sob métodos de pesquisa científica e investigação, com artifício de estatística e representação gráfica, serão evidenciados os processos acerca da Segurança da Informação, com ênfase no ambiente corporativo.

2. OBJETIVOS

2.1 Objetivo Geral

Serão conceituadas as manifestações empíricas e materiais da Segurança da Informação, com ênfase em suas aplicações no passado e da atualidade, dessarte os conceitos éticos e políticos desenvolvidos através da metodologia lógica e experimental.

2.2 Objetivo Específico

Destacar o funcionamento da Segurança da Informação no contexto corporativo, mediante a: influência de legislação relativa, organização empresarial, metodologia de operação de serviços e políticas de coleta de dados, assim como sua importância para o funcionamento das corporações.

3. JUSTIFICATIVA

A fim de perpetuar as atividades empresariais, as corporações sentem a iminente necessidade do investimento na Segurança da Informação, que tem por objetivo garantir proteção à base de dados da empresa e sobre os dados coletados de seus clientes. Este trabalho tem por fim, apresentar os moldes da segurança da informação, protegendo a base de dados, contornando riscos e adequando práticas da empresa às regulamentações, RGPD (Regulamento Geral sobre a Proteção de Dados) e LGPD (Lei Geral de Proteção de Dados Pessoais). Como propósito, a pesquisa visa oferecer propostas para a promoção da segurança do ambiente corporativo, tornando-o mais seguro e consistente.

4. O que são dados e informações para uma empresa

4.1 Tecnologias e suas ferramentas

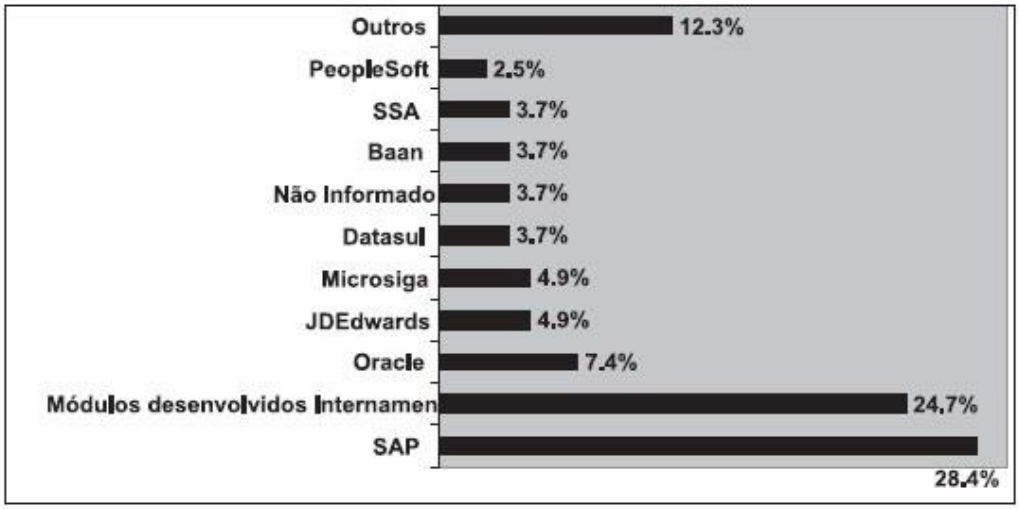
Dados são elementos como números, palavras ou medidores, que sozinhos não tem um significado específico, já as Informações, são dados que foram organizados e processados de maneira que tenha significado e relevância para um contexto específico. Em resumo, dados são os insumos, enquanto informações são o resultado da análise e interpretação desses insumos.

Davenport (2000) define os sistemas ERP(*Enterprise Resource Planning*) como pacotes de aplicações computacionais que dão suporte à maior parte das necessidades de informação das organizações, sendo derivado dos sistemas MRP (*Manufacturing Resource Planning*). O ERP se diferencia dos demais sistemas pela integração das informações da empresa, por meio do uso de um banco de dados único para toda a organização. Ele é composto de módulos integrados que atendem a cada área funcional ou processo, como Finanças, Produção, Custos, Vendas, RH etc.

Os Sistemas Integrados de Gestão, são uma das tecnologias mais utilizadas e discutidas na área de Sistemas de Informação, nos últimos anos (Bloomberg News, 2003). Delloite Consulting (1998) e Bernroider e Koch (1999) apontaram alguns dos principais resultados esperados com a adoção de sistemas ERP, tais como melhoria da qualidade e visibilidade da informação, maior integração e melhoria dos processos organizacionais, reduções de pessoal e reduções de inventário.

Tipos de ERPs utilizados por empresas:

Figura 2: Tipos de ERPs Utilizados pelas Empresas Pesquisadas



Mediante a pesquisas aprofundadas sobre o tema, foi revelado poucas contribuições do sistema ERP sobre as variáveis estratégicas Clientes e Consumidores, Rivalidade Competitiva e Mercado. O ERP demonstra agregar valor em relação à variável Fornecedores e à variável Produção, além disso oferece importantes contribuições para a Eficácia Organizacional e especialmente para a Eficiência Inter Organizacional. Entretanto, para atender a variáveis estratégicas relacionadas ao ambiente externo da organização (mercado, concorrentes, clientes/consumidores) conclui-se que é necessária a complementaridade de outros sistemas.

Você está em:

Relatório painel financeiro

Imprimir

Indústria Sucesso

Informações

Gerar relatório

Resultado	Jan/2016	Fev/2016	Mar/2016	Abr/2016	Mai/2016	Jun/2016	Jul/2016	Ago/2016	Set/2016	Out/2016	Nov/2016	Dez/2016	Total
Receita operacional bruta	133.757,89	108.417,71	123.897,48	92.405,72	49.846,33	0	0	0	0	0	0	0	508.325,13
[+] 10 - Receita	133.757,89	108.417,71	123.897,48	92.405,72	49.846,33	0	0	0	0	0	0	0	508.325,13
Custos de venda	-11.220,7	-5.900,2	-9.350,4	-4.263,71	-296,64	0	0	0	0	0	0	0	-31.031,65
[+] 20 - Impostos sobre a receita	-10.318,86	-5.474,42	-9.108,8	-3.859,98	-186,78	0	0	0	0	0	0	0	-28.748,84
21 - Crédito de impostos	0	0	0	0	0	0	0	0	0	0	0	0	0
23 - Fretes	-901,84	-425,78	-241,6	-603,73	-109,86	0	0	0	0	0	0	0	-2.282,81
(=) Receita operacional líquida	122.537,19	102.517,51	114.547,08	88.142,01	49.549,69	0	0	0	0	0	0	0	477.293,48
Receita operacional líquida (%)	91,61 %	94,56 %	92,45 %	95,39 %	99,40 %	%	%	%	%	%	%	%	93,90 %
Custos operacionais variáveis	-50.582,93	-35.751,29	-36.947,82	-18.307,2	-15.589,11	0	0	0	0	0	0	0	-157.178,35
30 - Matérias primas	-42.070,61	-30.782,7	-27.238,55	-16.793,95	-14.337,21	0	0	0	0	0	0	0	-131.203,02
31 - Embalagens	-8.036,42	-3.268,03	-8.755,67	-1.282	-1.087	0	0	0	0	0	0	0	-22.429,12
[+] 32 - Materiais de consumo operacionais	-475,9	-1.720,56	-953,6	-231,25	-164,9	0	0	0	0	0	0	0	-3.546,21
(=) Margem de contribuição	71.954,26	66.766,22	77.599,26	69.834,81	33.960,58	0	0	0	0	0	0	0	320.115,13
Margem de contribuição (%)	53,79 %	61,58 %	62,63 %	75,57 %	68,13 %	%	%	%	%	%	%	%	62,97 %
Custos e despesas operacionais	-80.217,61	-50.971,56	-76.248,11	-63.197,46	-51.440,16	0	0	0	0	0	0	0	-322.074,9
[+] 40 - Pessoal	-35.943,4	-33.919,58	-36.489,95	-34.521,56	-24.119,37	0	0	0	0	0	0	0	-164.993,86
[+] 41 - Infra-estrutura	-23.888	-1.545,95	-20.891,99	-15.169,76	-11.424,22	0	0	0	0	0	0	0	-72.919,92
[+] 42 - Serviços de apoio à operação	-5.566,12	-4.631,5	-6.565,98	-1.049,61	-3.906,3	0	0	0	0	0	0	0	-21.739,51
[+] 43 - Transporte próprio	-4.855	-4.075,1	-4.206,39	-3.303,97	-2.553,22	0	0	0	0	0	0	0	-18.993,68
[+] 44 - Marketing e vendas	-4.065,79	-341,75	-293,88	-154,2	-809	0	0	0	0	0	0	0	-5.664,62
[+] 45 - Despesas administrativas	-934,98	-380,05	-404,48	-546,71	-434,97	0	0	0	0	0	0	0	-2.701,19
[+] 46 - Manutenção	-693,1	-1.922,69	-150	-723,34	-608	0	0	0	0	0	0	0	-4.097,13
[+] 47 - Despesas financeiras	-4.271,22	-4.154,94	-7.225,44	-7.728,31	-7.585,08	0	0	0	0	0	0	0	-30.964,99
(=) Resultado operacional	-8.263,35	15.794,66	1.351,15	6.637,35	-17.479,58	0	0	0	0	0	0	0	-1.959,77
Resultado operacional (%)	-6,18 %	14,57 %	1,09 %	7,18 %	-35,07 %	%	%	%	%	%	%	%	-0,39 %
Variações de caixa não operacionais	2.836,41	-23.281,79	-6.004,21	-18.231,47	38.407,38	0	0	0	0	0	0	0	-6.273,68
[+] 50 - Atividades de investimento	-399,59	-176,57	-813,39	-782,71	-712,71	0	0	0	0	0	0	0	-2.884,97
[+] 51 - Atividades de financiamento	-17.065,33	-15.106,78	-5.390,82	-18.000,13	45.449,28	0	0	0	0	0	0	0	-10.113,78
[+] 52 - Aplicações financeiras	0,08	0	0	0,01	0,01	0	0	0	0	0	0	0	0,1
[+] 53 - Distribuição de lucros	0	0	0	0	-179,2	0	0	0	0	0	0	0	-179,2
[+] 54 - Ajustes de saldo	20.301,25	-7.998,44	0	551,36	-6.150	0	0	0	0	0	0	0	6.704,17
(=) Variação de caixa	-5.426,94	-7.487,13	-4.653,06	-11.594,12	20.927,8	0	0	0	0	0	0	0	-8.233,45
Variação de caixa (%)	-4,06 %	-6,91 %	-3,76 %	-12,55 %	41,98 %	%	%	%	%	%	%	%	-1,62 %

PAINEL FINANCEIRO

Você está em:

Itens da tabela de preço

Imprimir

Indústria Sucesso

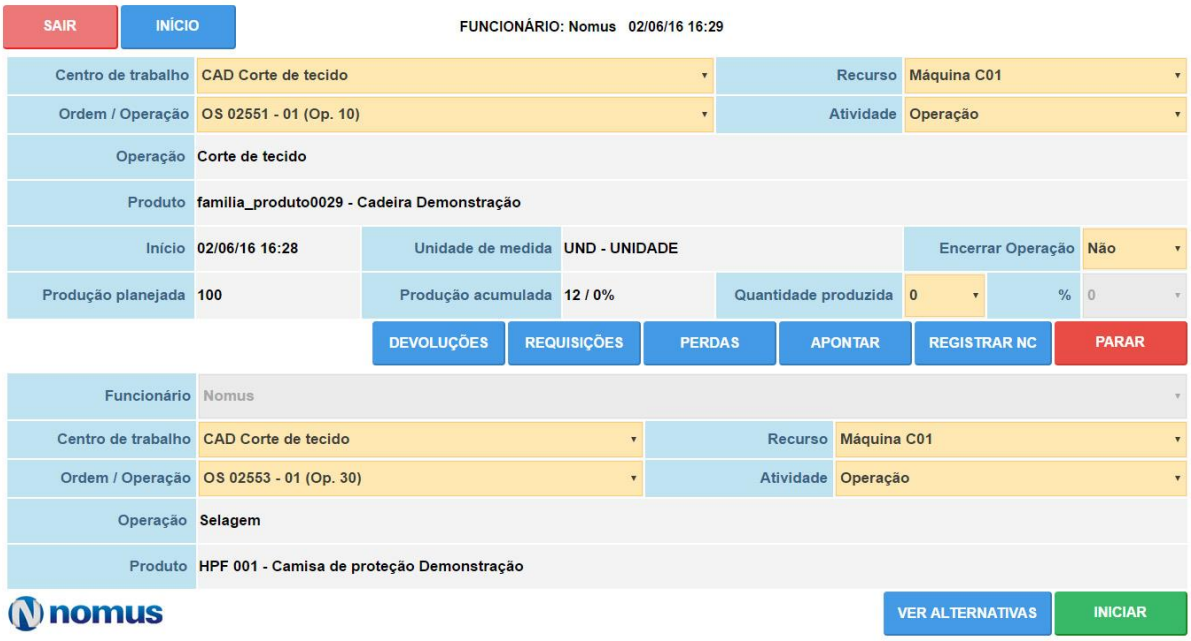
Código da tabela	Nome da tabela	Data/hora de criação	Data/hora do último cálculo	Usuário	Modelo de avaliação	Quantidade	Margem de lucro desejada	Empresa	Matriz	Observações
17	Tabela Treinamento 15-03-2016	15/03/16	15/03/16 11:34	Administrador Nomus	ICMS 19%	1.000	20,00	---	sim	---

Ordenar | Ações

Preço da tabela							Preço calculado pela análise de custos										Lucro previsto pela análise de custos		
	Seq	Código do produto	Descrição do produto	U.M.	Preço unitário	Preço unitário (U.M. secundária)	Lote de produção	Margem de lucro desejada (%)	Preço unitário calculado	Custos de venda	Custo de produção total	Custo de materiais	Custo de MOD	Custo CIF	Custos adm	Lucro líquido	Margem de contribuição		Lucro unitário previsto	Margem de lucro prevista (%)
☐		PL 128	Garrafa esportiva com válvula de segurança Demonstração	UND	15,00	---	500	20,00	30,26	10,80	0,50	0,04	0,24	0,22	12,91	6,05	19,42	🔴	-3,30	-22,03
☐		DR 004	Saco plástico Demonstração Fardo com 250 pacotes	Fardo	83,00	R$ 0,33 / PCT R$ 0,03 / Rolo	500	20,00	117,20	41,82	36,43	32,71	1,82	1,90	15,52	23,44	42,67	🟡	2,47	2,98
☐		AC 609	Piso Pav-stein 6 om Demonstração	METRO QUADRADO	55,00	---	1.000	20,00	52,31	18,66	9,61	8,16	1,21	0,25	13,57	10,46	25,49	🟢	12,11	22,02
☐		CAS 001	Agua mineral Cascatal 510ml sem gas Pack com 12 unidades Demonstração	PCT	198,00	---	300	20,00	198,39	70,79	69,98	69,75	0,01	0,21	17,95	39,68	57,86	🟢	39,44	19,92

Voltar | Cancelar

TABELA DE PREÇOS



TELA DE APONTAMENTO

Antes do CRM (*Customer Relationship Management*) ser implementado nas empresas, era utilizado o Marketing de Relacionamento que pode ser definido como "uma estratégia de marketing que visa construir uma relação duradoura entre cliente e fornecedor, baseada em confiança, colaboração, compromisso, parceria, investimentos e benefícios mútuos" (LIMEIRA, 2003). Surgiu então o CRM, *software* que evoluiu dos existentes. Ele é uma estratégia e um conjunto de ferramentas que as empresas utilizam para gerenciar e analisar as interações com clientes. O objetivo do CRM é melhorar o relacionamento com o cliente, aumentar a satisfação e fidelização, além de otimizar as vendas e o *marketing*.

> Se uma organização estiver procurando afinar todos os pontos de contato com a marca, integrando pessoas, processos e tecnologia do ponto de vista do cliente, resultando em valor de longo prazo para a marca, para a lealdade do cliente e rentabilidade, então pode-se ter certeza de que ela está entendendo o que significa CRM (LOBO, 2002).

Thompson (*apud* GREENBERG, 2001) aborda o CRM como um método "para selecionar e administrar os clientes, buscando otimizar o valor a longo prazo". Compendiando as definições acima, pode-se afirmar que CRM é a administração de uma estratégia que envolve toda a organização com o objetivo de atender bem seus clientes para trazer maiores lucros a longo prazo. Pode-se apontar, segundo Swift, (2001) pelo menos dois grandes benefícios, para a própria organização, com a implantação do CRM: primeiramente, em decorrência de produtos mais

convenientes e clientes mais satisfeitos, além da preocupação e carinho demonstrado, que aumentam a lealdade e confiança, consequentemente serão obtidas maiores receitas; em segundo lugar geram-se menores custos, pois os esforços e verbas são mais direcionados, o que melhora muito a alocação de recursos e eficiência da empresa.

4.2 A importância do banco de dados

O banco de dados para o contexto de uma organização possibilita e muito a segurança das informações, logo, no que permite ao público-alvo certa credibilidade aos dados pessoais dos quais transmitidos são a organização. O armazenamento de dados quanto informações precisas ao público-alvo facilita e muito a organização no que tange uso de estratégias e, isto, visando melhorias ao atendimento e, contudo, alcance as necessidades de consumo que presente se tem por cada indivíduo.

Os dados de um banco relacional têm semelhança a uma estrutura de tabela utilizando linhas e colunas para distinguir os dados e uma chave primária para localizar os dados e até realizar relações com outras tabelas que, por sua vez, proporciona certa organização e segurança nos dados. Todas as empresas buscam tecnologias para facilitar a manipulação de dados e, no entanto, o banco de dados é o mais apropriado para essa função. Desse modo, desenvolvido para armazenamento de grande quantidade de dados e, com isso, permite o usuário buscar as informações armazenadas no mesmo de forma rápida e prática

Com isso, evidencia-se que o banco de dados é uma ferramenta fundamental para serviços e negócios na web, que pode trazer uma busca organizada, em tempo real e totalmente segura, por isso, as organizações e até os profissionais autônomos buscam cada vez mais conhecimento na linguagem SQL(*Structured Query Language*) para arquitetar uma busca e um retorno das informações. Agora, o que assim é importante validar é que: “[...] a proteção das informações tornou-se condição [...] à manutenção da competitividade organizacional”.

É diante da articulação entre uma informação assegurada de proteção e potencialização aos negócios que verifica certa relevância. E, isto, é de grande possibilidade por questões dos “[...] bancos de dados, conterem dados e informações que podem agregar valor ao negócio e propiciar as condições necessárias à obtenção do diferencial e da vantagem competitiva [...]” (SILVA; ROSA, 2017, p.66).

5. Evolução da segurança dos dados

5.1 Histórico da segurança de dados

Hoje em dia é muito comum falar sobre segurança de informação, porém é difícil afirmar com exatidão quando a segurança de dados começou a ser uma preocupação. Acredite ou não, mas os primeiros usos da criptografia, por exemplo, são constantemente atribuídos aos hebreus em 600 a.C. Eles utilizaram a Cifra de César uma cifra de substituição simples para escrever o Livro de Jeremias.

Posteriormente, na primeira e segunda Guerras Mundiais, a criptografia também teve um papel importantíssimo para proteger a comunicação e a troca de informações sigilosas entre os países que batalhavam entre si. Foi nessa época que duas grandes máquinas de cifragem e decifragem surgiram: a alemã Enigma, patenteada por Arthur Scherbius, e a Máquina de Turing, desenvolvida pelo britânico Alan Turing. Essa última, elaborada pelo “pai da informática”, era usada para decifrar as mensagens alemãs e ganhar vantagem no conflito.

De acordo com o governo, e a Lei Geral de Proteção de Dados (LGPD), por volta da década de 70

> O primórdio da nova cultura de proteção de dados aconteceu na década de 70, na Alemanha, devido ao avanço da computação e da premente e constante preocupação do Estado Alemão para proteger seus cidadãos do que a nação vivenciou no período do regime nazista. Dessa forma, foram criadas as primeiras normas regulatórias que culminaram na legislação de 1978.

5.2 Criptografia de ponta a ponta, comunicações modernas

Segundo a empresa global de tecnologia IBM: “A criptografia de ponta a ponta (E2EE) é um processo de comunicação seguro que criptografa dados antes de transferi-los para outro *endpoint*. Os dados permanecem criptografados durante o trânsito e são descriptografados no dispositivo do destinatário.” (IBM 2024)

Criptografia de dados consiste no processo de usar um algoritmo que converte os caracteres de texto padrão em um formato ilegível. Usada para privacidade incluem assuntos sensíveis como documentos de negócios, detalhes financeiros, procedimentos legais, prontuário médico e conversas pessoais. Consequentemente, a falha em proteger os dados privados pode resultar em danos às empresas e seus clientes. Comumente utilizada em sistema de chat, onde à troca de mensagens.

A criptografia é uma maneira de proteger dados ao transformar textos de formatos simples em cifras, esses dados precisam de uma “chave de segurança” para serem legíveis, o que proporciona maior segurança aos dados.

Essa tecnologia usa a segurança cibernética para proteger contra ataques de força bruta e cibernéticos, como o *malware*(*software* malicioso), ela protege os dados transmitidos na nuvem e em sistemas de computador. Existem dois tipos de dados digitais, os transmitidos ou em trânsito e os dados armazenados ou em repouso.

5.3 Surgimento de *malware* e os primeiros antivírus

O ano de 1971 foi um marco significativo na história da cibersegurança com o surgimento do primeiro *malware* conhecido como “*Creeper*", criado por Bob Thomas. O *Creeper*, na verdade, não tinha a intenção de causar danos aos sistemas. Em vez disso, ele era uma espécie de experimento e, de certa forma, uma demonstração de como um programa poderia se espalhar através de uma rede. Conforme a tecnologia avançava, os *malwares* se tornavam cada vez mais sofisticados. Eles deixaram de ser simples brincadeiras para se transformarem em armas poderosas nas mãos de criminosos cibernéticos. A década de 2000 trouxe os *ransomwares* (tipo de *malware* que bloqueia o computador e exige um resgate para desbloqueá-lo.), que se tornaram um pesadelo para empresas e usuários comuns.

Hoje, *malwares* continuam a evoluir a uma taxa alarmante e cada vez mais as empresas de todos os tamanhos enfrentam ameaças constantes.

A resposta ao Creeper veio logo depois, com o desenvolvimento do primeiro antivírus, conhecido como “*Reaper,*” criado por Ray Tomlinson,em 1972 . O *Reaper* capturava e removia o *Creeper* dos sistemas afetados. O funcionamento do *Reaper* era semelhante ao funcionamento do *Creeper*, mas, ao invés de apresentar mensagens na tela, ele se replicava e espalhava na rede com o objetivo de apagar cada *Creeper* que existia.

Naquela época, essa dinâmica não teve muita atenção, afinal, não houve uma grande ameaça. Porém, a partir da década de 80, há uma mudança: com o maior alcance da Internet e com mais pessoas acessando computadores, começaram a surgir vírus maliciosos, com objetivo de causar dano e roubar dados.
Apesar disso, os vírus nunca foram a única preocupação da segurança de informação naquele tempo. Pessoas sem autorização alcançando dados sensíveis

ou lendo documentos que não deveriam também causavam grandes estragos nos primórdios da computação e internet.

Segundo o autor Flávio Motta Coutinho os antivírus são uma parte importante da vida de todos os cidadãos - já que é a grande maioria da população mundial está conectada. Portanto é importante não negligenciar o uso dos *softwares* para garantir a sua segurança.

6. A importância da segurança de dados

6.1 A segurança da informação no ambiente de trabalho

Na atualidade, dentro do ramo empresarial, a segurança da informação é essencial. As transações comerciais estão cada vez mais digitalizadas, abrindo margem para riscos de violações de dados e ataques cibernéticos, que representam uma grande ameaça às empresas. Dos clientes e funcionários, até a corporação, os dados são muito preciosos, onde a segurança informacional desempenha um papel fundamental na consolidação e construção da empresa, tanto por sua credibilidade quanto pela confiança.

“A prevenção reputacional em empresas que adotam soluções tecnológicas de segurança da informação traz uma série de benefícios interessantes.” (OTENN, 2024). As empresas que seguem normas legislativas, sobre a segurança de dados, protegem a credibilidade da clientela e dos associados, preservando esse relacionamento, que é essencial para o sucesso da empresa. A credibilidade ajuda com a atratividade dos serviços para os clientes, mantendo os já existentes, isto em um cenário onde as pessoas estão cada vez mais conscientes de como é importante manter os seus dados particulares seguros.

Manter a credibilidade da marca é essencial para seu sustento a longo prazo de empreendimento, empresas com imagens marcadas por invasão ou vazamentos de dados, enfrentam dificuldades para tentar continuar no mercado ou até voltar ao seu espaço conquistado no mesmo.

A segurança da informação insere medidas e tecnologias que ajudam a proteger os dados, onde, umas das tecnologias usadas é a *cloud computing* (sistema de computação em nuvem) que oferece diversos benefícios às empresas, que pagam pelo direito de uso destes serviços, que fornecem uma camada de proteção aos dados da empresa. Com o salvamento da nuvem oferecido pelo *cloud computing* os dados estão mais seguros, devido a uma criptografia de ponta a ponta somada ao monitoramento de dados. Essas tecnologias ajudam a proteger contra

vazamentos de dados, adulterações e ataques cibernéticos, obtendo uma confidencialidade dos dados.

Com cada vez mais tecnologia presente, a segurança no ambiente corporativo sofre com a necessidade de adaptação, com *hackers* mais experientes, que acabam buscando dados chave para a empresa, dados pessoais de seus clientes. Os mesmos também devem incrementar medidas que conscientizem os trabalhadores e os clientes a não caírem em golpes como: *Malware, Phishing* e Injeção de SQL.

6.2 Criptografia de dados

De acordo com Kaspersky: A criptografia é a conversão de dados para um formato codificado, no qual os mesmos só poderão ser acessados, após serem descriptografados. A criptografia é fundamental para proteger os dados de clientes de uma empresa, da própria empresa e de uma pessoa normal.

Quando compartilham algo na internet esses dados ou informações, passam pela rede pública correndo o risco de serem roubados por *hackers.* Para evitar esse possível acontecimento os mesmos podem instalar um *software* ou *hardware*, para criptografar esses dados tornando muito mais difícil obter essas informações.

“Apenas criptografar cegamente todos os dados não é seguro. Se você colocar muita ênfase na segurança e usar criptografia que cause transtornos aos usuários, isso poderá afetar seus negócios da mesma forma.” (TECNEWS.NET)

Para a empresa a criptografia é algo essencial, pois com essa segurança os clientes se sentem bem mais seguros sobre os seus dados. Manter dados criptografados ajuda a empresa a manter as próprias transações, dados e ter conversas muito mais seguras, aumentando a sua própria confiabilidade no mercado, aumentando a chance de clientes e fornecedores em potencial.

Temos um ótimo exemplo sobre o que ocorreu em setembro de 2018 com o *Facebook*, com o vazamento das informações de aproximadamente 87 milhões de usuários, a empresa foi processada em R$20 milhões em danos morais e R$5 mil para cada usuário que entrasse com uma ação contra a empresa. Esse escândalo trouxe uma dúvida para milhões de pessoas, será que o *facebook* ainda é confiável? Mas após o período de reformulação sobre a política de privacidade e as desculpas de seu criador (Mark Zuckerberg), o *Facebook* conseguiu se reerguer.

Assim como o sistema de criptografia de ponta a ponta do *whatsapp*, que apenas os participantes da conversa podem lê-las e saber o que está escrito, sendo

uma criptografia ‘’simples’’ sendo de fácil descriptografar pois o próprio *whatsapp* faz isso por você. Aumentando a confiança dos usuários e melhorando a credibilidade do aplicativo, tornar os dados dos usuários mais seguros é essencial para que o aplicativo continue crescendo no mercado.

7. Política de coleta de dados

7.1 Introdução a política de coleta de dados

Na era digital, os avanços tecnológicos transformaram os dados pessoais em ativos estratégicos de grande valor econômico para empresas públicas e privadas. Essa valorização dos dados trouxe consigo a necessidade de regulamentação e de um controle mais rigoroso sobre sua coleta, tratamento e uso. Em resposta a essa demanda, diversos países implementaram legislações específicas para proteger os titulares e regulamentar o tratamento das informações pessoais. No Brasil, a Lei Geral de Proteção de Dados (LGPD) reflete essa necessidade, estipulando diretrizes para assegurar que as informações sejam coletadas e utilizadas de maneira responsável e transparente, estabelecendo a proteção dos dados como uma prioridade central para todas as organizações (Almeida; Soares, 2022).

Diante desse contexto, Almeida e Soares (2022) consideram que uma política de coleta de dados eficaz deve esclarecer de maneira específica e acessível quais informações serão coletadas, a finalidade da coleta e o modo como os dados serão tratados e armazenados. Além de atender às exigências legais, a política deve considerar o consentimento informado do titular, que precisa estar plenamente ciente do propósito e do alcance do uso de seus dados. Essa transparência reforça a confiança dos clientes e usuários e garante que o processo de coleta e tratamento seja conduzido de forma ética, evitando práticas abusivas e promovendo uma cultura de segurança da informação.

A LGPD assegura aos consumidores o direito de acessar, corrigir, restringir e excluir seus dados pessoais, reforçando a privacidade. Ao se elaborar uma política de coleta de dados devem ser observados alguns pontos, dentre os quais destacam-se:

a) consentimento claro: o usuário deve dar permissão explícita para a coleta de dados, sem formulários ambíguos ou ocultos;

b) direito de remoção e transferência: o usuário pode solicitar a exclusão ou transferência de seus dados a qualquer momento, sem justificativa;
c) responsabilidade: a empresa é responsável pelos dados coletados e responde legalmente por vazamentos ou uso indevido;
d) uso de *cookies*: o rastreamento de dados só pode ocorrer com consentimento expresso, garantindo necessidade, adequação e proporcionalidade (Sebrae, 2023).

A política de coleta de dados precisa incluir medidas que assegurem a proteção e a segurança das informações coletadas, como o controle de acesso rigoroso e a manutenção de registros detalhados sobre o tratamento dos dados. Esses registros contribuem para a rastreabilidade das atividades realizadas e para a prestação de contas diante de possíveis auditorias e investigações de irregularidades, sendo fundamentais para a governança e o *compliance* organizacional. Dessa forma, a política de coleta de dados se torna um componente central na gestão de dados de qualquer organização, ao mesmo tempo em que protege o titular e fortalece a integridade e a responsabilidade da empresa (Almeida; Soares, 2022).

7.2 Controle de acesso

O controle de acesso define os direitos de usuários para que cada um acesse apenas os recursos previamente autorizados no sistema, como funcionalidades, arquivos ou sistemas. Esse processo permite ou nega o acesso de um sujeito (usuário, processo ou sistema) a um objeto específico, reduzindo significativamente os riscos à segurança da informação e ajudando a preservar a continuidade das operações empresariais, embora não elimine completamente as ameaças (Barreto *et al.,* 2018).

Machado (2014) explica que o controle de acesso foca na identificação e autenticidade do usuário que se conecta a uma rede. Primeiro, é necessário verificar se o usuário é quem afirma ser e, em seguida, se possui as credenciais e permissões necessárias para acessar os recursos. A identificação assegura que um sujeito (usuário, programa ou processo) é autenticado por meio de uma credencial, que pode incluir nome de usuário, PIN, *smart card*, assinatura digital ou característica biométrica, como impressão digital. Para completar a autenticação, o

usuário geralmente deve fornecer uma segunda forma de validação, formando um conjunto seguro de credenciais.

De acordo com a Autoridade Nacional de Proteção de Dados (ANPD, 2021) o controle de acesso é uma medida técnica que assegura que apenas pessoas autorizadas possam acessar dados sensíveis, protegendo a integridade das informações. Baseia em três processos principais:

- autenticação: identifica o usuário que acessa o sistema ou os dados;
- autorização: define as ações permitidas para o usuário autenticado;
- auditoria: registra e monitora as atividades realizadas pelo usuário, permitindo rastrear alterações e acessos.

Esses processos em conjunto reforçam a segurança e a conformidade com as políticas de privacidade e proteção de dados (ANPD, 2021).

7.3 Impacto e avaliação de risco

Com o avanço dos sistemas de informação, comércio eletrônico e tecnologias digitais, empresas e indivíduos se deparam com riscos crescentes de fraudes e ameaças, tornando a segurança da informação indispensável para proteger dados e sistemas. Além de preservar a integridade e a confiabilidade das informações, a segurança da informação tornou-se um pilar estratégico crucial para a competitividade e sustentabilidade das organizações. Em um ambiente cada vez mais digital, a exposição a ataques pode comprometer operações, gerar prejuízos financeiros e afetar seriamente a imagem da empresa, exigindo medidas robustas de proteção e prevenção (Machado, 2014).

Segundo Barreto *et al.* (2018), diversos tipos de incidentes podem atingir empresas de todos os portes, desde o roubo de informações confidenciais e vazamentos de dados de clientes até sequestros digitais e interrupções operacionais. Assim, compreender esses riscos é fundamental para que as empresas possam adotar políticas e práticas robustas de proteção para mitigar impactos negativos em seus negócios e na relação com seus clientes. Dentre os principais riscos para os dados destacam-se:

a) roubo de informações confidenciais: o maior ativo de muitas empresas é o conhecimento sobre como operam, como no caso de uma receita secreta que garante vantagem competitiva. Se essa informação for exposta, a empresa perde seu diferencial no mercado;

b) impacto na operação: muitas empresas dependem de sistemas digitais. Uma invasão que paralise esses sistemas, mesmo por um curto período, pode gerar prejuízos financeiros, afetar operações e abalar a confiança dos clientes;

c) sequestro de dados: em casos de invasão, dados essenciais podem ser sequestrados e usados como extorsão, levando a empresa a pagar grandes somas para recuperá-los;

d) vazamento de dados confidenciais de clientes: quando dados pessoais, como documentos e informações financeiras, são expostos, a empresa falha em seu compromisso de proteger esses dados, o que pode resultar em sanções legais e perda de confiança;

e) danos à imagem: a ocorrência de qualquer um desses problemas abala a confiança dos clientes, impactando a reputação da empresa e podendo levar à perda de clientes e a prejuízos financeiros significativos (Barreto *et al,* 2018).

8. Ética na segurança de dados

8.1 Qual o dever da ética?

Sobre a ética temos “[...] a ética é a investigação sobre aquilo que é valioso, ou sobre aquilo que é realmente importante [...]” (Wittgenstein, p. 41, 2015), desta forma, podemos entender que a ética seria o questionamento de ações e atitudes acerca das interações no meio social. Em ambientes corporativos a presença da ética é fundamental para a manipulação de informações e dados pessoais.

Organizações possuem o compromisso legal de garantir a integridade e a privacidade de dados de pessoas naturais, e para que isso ocorra de maneira correta, medidas de proteção devem ser aplicadas de acordo com Lima (2024).

> [...] As organizações devem ser transparentes em relação às suas práticas, isso inclui fornecer informações claras sobre como os dados são coletados, armazenados, usados e protegidos, além de notificar os usuários sobre quaisquer incidentes de segurança que possam afetá-los. (Lourenço, [2024])

No setor contemporâneo dados e informações são valiosas para as empresas, quanto mais elas possuírem, mais benéfico, por tal motivo, diversas situações como o vazamento de dados, são frequentes, principalmente em

softwares de código fechado. Para Lima, um exemplo significativo seria a aquisição de dados pessoais para determinadas causas, e partindo destas as utilizarem para fins que diferem de suas motivações iniciais, sendo este a demonstração de uma situação em que o conceito ético não foi aplicado.

E para que tais informações recebam o devido tratamento, algumas premissas devem ser seguidas, como as de honrar os direitos de propriedade, respeitar a privacidade de terceiros, e assegurar a consistência assim como a integridade da informação dita (Oliveira, [2024]).

8.2 Atuação da ética na cibersegurança

A aplicação da ética na cibersegurança nada mais é do que:

> [...] um conjunto de princípios e valores que guiam as ações dos profissionais de segurança digital em seu trabalho. Esses princípios determinam o que é considerado aceitável, honesto e justo ao lidar com sistemas, dados e privacidade. A ética exige que os profissionais considerem o impacto de suas ações em indivíduos, organizações e na sociedade como um todo. (Moraes, 2024)

Dessa forma podemos pontuar que atuação ética em empresas é fundamental, para a construção de um ambiente digital mais seguro e confiável. E para Moraes (2024) algumas práticas que podem assegurar a ética na cibersegurança são: Definir e seguir um Código de Conduta; Educação e Treinamento em Ética; Transparência nas Ações; Compromisso com a Divulgação Responsável; Respeito aos Direitos dos Usuários; Adesão a Padrões e Regulamentos. Tais medidas possibilitam maior segurança e confiança em empresas que necessitam de dados particulares para oferecerem seus produtos ou serviços.

Dito isso, as organizações precisam levar em consideração a moralidade de seus consumidores, e não apenas o que se pode fazer ou o que a regulamentação permite (Sebrae, [2024]). Logo, empresas precisam criar um equilíbrio entre ações, aquilo que lhes é favorável e o eticamente correto a se realizar.

> É vital que o setor corporativo continue a promover e praticar uma forte ética no tratamento dos dados pessoais. Isso inclui não apenas ações proativas para educar e alertar clientes e usuários sobre potenciais golpes, mas também um compromisso contínuo com o entendimento responsável do

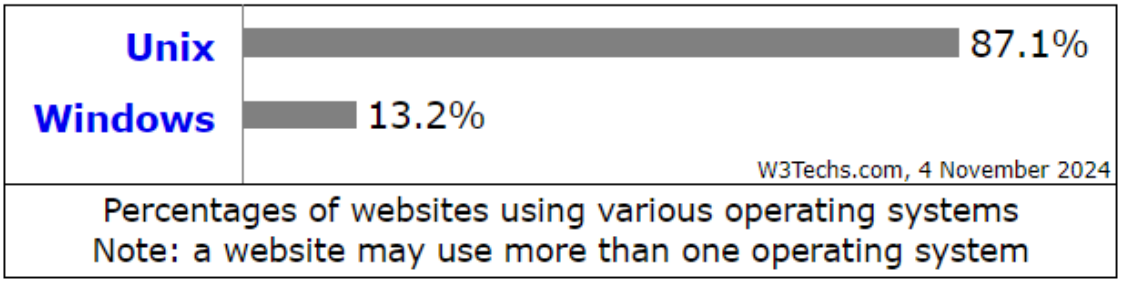
> ciclo completo de vida dos dados pessoais, desde a coleta até a eliminação. (Lima, 2024)

Portanto, podemos concluir que conforme ocorre o aumento da transparência, responsabilidade e acessibilidade, práticas como a documentação e a revisão de dados são aconselhadas ao manusear dados particulares colhidos por empresas segundo Cepelak (2024). Desse modo é necessário que, entidades que utilizam informações derivadas de pessoas naturais certifiquem-se e invistam no manejo correto e ético destas informações.

CONCLUSÃO

Sobre o atual cenário, dessarte as análises e pesquisas discutidas neste trabalho, com a necessidade de encriptação dos sistemas de armazenamento de dados, faz-se necessário questionar os cotidianos usos de *softwares* proprietários e suas falhas encriptações de dados, substituindo-as por *softwares* livres e de código aberto, com destaque naqueles capazes de permitir maiores configurabilidades voltadas para os relativos à segurança.

Observável é a imposição do uso de *softwares* de empresas privadas, em sua maioria, *big techs*, empresas que têm hegemonia do mercado e que o moldam a partir de suas necessidades. Por exemplo, os sistemas operacionais *Windows* e *Mac* são ainda usados amplamente por empresas no mundo, porém, estes sofrem de sérios problemas com encriptação e vazamento de dados, por conta de sua natureza e do amplo uso de *softwares* proprietários, portanto, como tendência de mercado, se faz cada vez mais presente o movimento *open source* (código aberto) e o de *softwares* livres, como os sistemas baseados em *Unix*, o *Linux* e suas distribuições, assim como o *BSD (Berkeley Software Distribution)* e seus derivados, acrescentando destaques para os sistemas *OpenBSD*, que são, por muitos especialistas, considerado o sistema mais seguro contra ataques *hacker*, *DDoS* (*Distributed Denial of Service*, que em português significa "Negação de Serviço Distribuída"). É um tipo de ataque cibernético que consiste em sobrecarregar um servidor, *website* ou recurso de rede com tráfego malicioso. O objetivo é interromper o tráfego normal e tornar o alvo indisponível para os usuários), *Malwares* (termo genérico para qualquer tipo de *software* malicioso que pode prejudicar um computador ou dispositivo) e o *Doxing* (*Doxing*, ou *doxxing*, é a prática virtual de pesquisar e de transmitir dados privados sobre um indivíduo ou organização), onde, junto com as outras distribuições *BSD* e *Linux*, formam o sustentáculo da segurança digital em servidores a nível global, exemplificado na discrepância quantitativa entre *Unix based systems* (sistemas baseados em *Unix),* tal que, o site *W3techs* realizou um estudo em novembro de 2024 que aponta que 87,1% dos servidores de todo o mundo usa sistemas baseados em *Unix,* segue o gráfico:



Percentages of websites using various operating systems
Note: a website may use more than one operating system

Além da desinformação tecnológica, com relação a uso de *softwares*, um dos coeficientes agravantes na insegurança do usuário com relação a coleta de dados, mediante cenário de capitalismo informacional e mundo globalizado, são a permissividade por parte dos gestores políticos para com tal quadro, de maneira que, as empresas, com ênfase nas *Big Techs*, identificados na materialidade, vários casos de tráfico de dados pessoais, tal qual a notícia do site Olhar Digital evidencia:

> Grandes empresas de tecnologia, como Google, Meta e Microsoft, estão no centro de uma preocupante prática que envolve o uso dos dados pessoais de seus usuários para treinar suas inteligências artificiais. Essas corporações coletam conversas, fotos e documentos de milhões de indivíduos, com o intuito de alimentar suas IA, capacitando-as a realizar desde tarefas de escrita até a criação artística. [...]

Dessarte, entende-se a necessidade ao reforço legislativo e ao compromisso político dos responsáveis no Estado, a nível Nacional (Brasil), requerem-se alterações na LGPD, para que esta se distancie de um “acordo comercial” e torne-se um objeto de autoridade e regulamentação. Assim como, cabe ao usuário também tomar consciência da realidade da qual ele participa, identificar a falta de inocência na simplicidade ao qual este é submetido à assinatura de um termo de uso de um *software*, da qual, frequentemente sequer foi lida ou minimamente compreendida. Em cenário mundial, as relações do compromisso de proteção aos dados do usuário, possuem moldes diversos que configuram certa complexidade, logo, cabe a luta política de determinada população para aquisição de seus interesses, assim como seu processo de auto reconhecimento, de pesquisa e estudo sobre como o usuário pode acessar *softwares* isento dos interesses de terceiros e cada vez mais, ganhar identidade e força em um cenário social ainda não desbravado, o cenário informacional. A tendência é, cada vez mais, os usuários reivindicarem-se como indivíduos, ao invés da permanência como produto de comercialização informacional.

REFERÊNCIAS

ALMEIDA, S. do C. D. de; SOARES, T. A. **Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital**. Perspectivas em Ciência da Informação, v. 27, n. 3, p. 26–45, jul. 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/?format=pdf&lang=pt. Acesso em: 27 out. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**: versão 1.0. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 14 de out. 2024.

BARRETO, J. *et al.* **Fundamentos de segurança da informação**. Porto Alegre: SAGAH, 2018.

BRASIL. **Decreto-lei nº 13.709**, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.ht .Acesso em: 14 out. 2024.

BRASIL. Decreto-lei nº 13.709, de 14 de agosto de 2018. Dos requisitos para o tratamento de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 out. 2024.

CEPELAK, C. **Uma introdução a ética de dados: O que é o uso ético dos dados?**. Datacamp. Publicado em: 23 de abril de 2024. Disponível em: https://www.datacamp.com/pt/blog/introduction-to-data-ethics. Acesso em: 16 set. 2024.

Sebrae. **Como aplicar a ética digital no seu negócio?**. [2024]. Disponível em: https://sebrae.com.br/sites/PortalSebrae/artigos/como-aplicar-a-etica-digital-no-seu-negocio,bddbaa85f0b25810VgnVCM100000d701210aRCRD. Acesso em: 16 set. 2024.

DUQUE, J.M.PEREIRA. **Adoção de CRM nas Autarquias Locais**. 2009. Disponível em: https://repositorio.utad.pt/entities/publication/54a5dfbe-ed04-4717-ae52-aceb92364506. Acesso em: 16 set. 2024.

EACH.USP. **Segurança da Informação: O primeiro vírus e o desenvolvimento da área.** 2024. Disponível em: https://www.each.usp.br/petsi/jornal/?p=2896#:~:text=Reaper%3A%20o%20primeiro%20antiv%C3%ADrus,Creeper%20dos%20computadores%20na%20ARPANET. Acesso em: 25 nov. 2024.

GAEA. **Criptografia de dados: entenda como realizar na sua empresa**. 2021. Disponivel em: https://gaea.com.br/criptografia-de-dados/#:~:text=O%20uso%20da%20criptografia%20de,de%20redes%20devem%20ser%20criptografados

Acesso em: 16 set. 2024.

GOV.BR. **Lei Geral de Proteção de Dados.** (2024). Disponível em: https://lgpd.df.gov.br/historico/#top. Acesso em: 18 nov. 2024

GUARDSI. **A história dos malwares**. 2023. Disponível em: https://blog.guardsi.com.br/a-historia-dos-malwares/#:~:text=Em%201971%20foi%20um%20marco,software%20malicioso%20era%20praticamente%20desconhecida https://www.docusign.com/pt-br/blog/importancia-seguranca-da-informacao. Acesso em: 18 nov. 2024.

GUIMARÃES, Tomás de Aquino. **Tipos de ERPs Utilizados pelas empresas pesquisadas**. 2009. Disponível em: https://www.scielo.br/j/rac/a/MhrBC7F4BqqX9W3BgH4P5TN/#. Acesso em: 26 nov. 2024.

IBM. **O que é criptografia de ponta a ponta (E2EE)?**. 2023. Disponível em: https://www.ibm.com/br-pt/topics/end-to-end-encryption. Acesso em: 25 nov. 2024.

KSPERSKY**. O que é criptografia de dados? Definição e explicação.** [2024]. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em: 25 nov. 2024.

LEÃO, Thiago. **Exemplo de ERP: Tela de apontamento, Tabela de preços e Painel Financeiro**. 2024. Disponível em: https://www.nomus.com.br/blog-industrial/erp/. Acesso em: 26 nov. 2024.

LIMA, A. **A ética na proteção de dados na era digital** - Priorizando o humano no mundo digital**.** Migalhas. 2024. Disponível em: https://www.migalhas.com.br/depeso/400225/a-etica-na-protecao-de-dados-na-era-digital. Acesso em: 25 nov. 2024.

LOURENÇO, M. **Ética e Aspectos Jurídicos em Cibersegurança.** E-Safer. [2024]. Disponível em: https://e-safer.com.br/etica-e-aspectos-juridicos-em-ciberseguranca/#. Acesso em: 25 nov.2024.

MACHADO, F. N. R. **Segurança da informação: princípios e controle de ameaças**. Rio de Janeiro: Érica, 2014.

MICROSOFT. **Contrato de Serviços Microsoft.** 2023. Disponível em: https://www.microsoft.com/pt-br/servicesagreement. Acesso em: 25 nov. 2024.

MORAES, L. C. de. **O papel da ética na cibersegurança.** Dolutech. 2024. Disponível em: https://dolutech.com/o-papel-da-etica-na-ciberseguranca-entenda/. Acesso em: 26 ago. 2024.

OLIVEIRA, P. A. A. de. **Segurança, Privacidade, Questões Éticas em Sistemas de Informação e seus Impactos Sociais.** [2024]. Disponível em: https://www.inesul.edu.br/professor/arquivos_alunos/doc_1405106051.pdf. Acesso em: 11 nov. 2024.

PERALLIS. **A história da segurança da informação: mais de um século protegendo conhecimento.** (2024). Disponível em:https://www.perallis.com/news/a-

historia-da-seguranca-da-informacao-mais-de-um-seculo-protegendo-conhecimento. Acesso em: 25 nov. 2024.

SEBRAE. **LGPD: aprenda a realizar a coleta de dados de forma segura e legal**. 2023. Disponível em: https://sebrae.com.br/sites/PortalSebrae/artigos/lgpd-aprenda-a-realizar-a-coleta-de-dados-de-forma-segura-e-legal,b10743ad7fe96810VgnVCM1000001b00320aRCRD. Acesso em: 25 nov. 2024.

SNOWDEN, EDWARD. **Edward Snowden:** “The problem isn't data protection; the problem is data collection”**.** 2019. Disponível em: https://verdict-encrypt.nridigital.com/verdict_encrypt_winter19/edward_snowden_data_protection_collection_gdpr. Acesso em: 27 out. 2024.

TECMUNDO. **Afinal, como surgiu o primeiro vírus e o antivírus da computação?**. 2023. Disponível em: https://www.tecmundo.com.br/seguranca/260332-surgiu-primeiro-virus-o-antivirus-computacao.htm. Acesso em: 27 out. 2024.

W3TECHS. **Usage statistics and market shares of operating systems for websites.** 2024. Disponível em: https://w3techs.com/technologies/overview/operating_system. Acesso em: 25 nov. 2024.

WITTGENSTEIN, L. Uma conferência sobre ética. Tradução: Leonel Lucas Azevedo e Mário Jorge de Carvalho. Imprensa da Universidade de Coimbra. 2015.