Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS
ISSN 2358-4432


SEGUNDA FASE SEGURANÇA DA INFORMAÇÃO E LGPD APLICADO NO DESENVOLVIMENTO DE SOFTWARE GOVERNO ELETRÔNICO

SECOND PHASE INFORMATION SECURITY AND LGPD APPLIED IN SOFTWARE DEVELOPMENT OF ELECTRONIC GOVERNMENT

Fábio Alexandrini,
Doutor e Mestre em Engenharia de Produção e Sistemas, Bacharel em Ciência da Computação
Professor EBTT IFC – Rio do SUL/ fabio.alexandrini@ifc.edu.br

Cleber Nardelli
Especialista em Desenvolvimento Web e Engenharia de Software, Bacharel em Sistemas de Informação. Professor Unidavi/ cleber.nardelli@gmail.com

Resumo:
As práticas adotadas em uma empresa de desenvolvimento de software, relacionadas à Segurança da Informação e LGPD (Lei Geral de Proteção de Dados), na construção e manutenção de aplicações seguras em e-government. O Estudo de caso (pesquisa qualitativa) foi realizado em uma empresa que desenvolve Sistemas de Gestão e Governo Eletrônico ficando explicita a necessidade de adoção de práticas relacionadas a segurança da informação para que estivesse aderente aos requisitos da Lei 13.709/2018-LGPD. A coleta de dados realizou-se diretamente no ambiente no qual a aplicação das práticas foram observadas. A partir dessa observação das práticas de segurança, um modelo temático foi elaborado tendo como eixos: Técnico, Cultural/Pessoal e Jurídico, em seguida para cada eixo uma subdivisão em áreas mais específicas fora realizada, obtendo-se como resultado as seguintes áreas: Desenvolvimento, Produto e TIC (no eixo Técnico), Interno e Externo (no eixo Cultural/Pessoal) Ao todo foram identificadas 42 práticas em uso, sendo algumas adotadas exclusivamente pelo advento de segurança com foco na LGPD e outras já existiam, sendo modificadas como necessário. Por fim, todas as práticas foram descritas de maneira individual. Nesse artigo foram abordadas as demais práticas analisadas e que essas possam contribuir e auxiliar outras instituições públicas e privadas na adoção delas no ambiente de desenvolvimento de software.
Palavras-chave: governo eletrônico, LGPD, soluções tecnológicas de gestão, tecnologia da informação e comunicação, segurança da informação.

Abstract:
The practices adopted in a software development company, related to Information Security and LGPD (General Data Protection Law), in the construction and maintenance of secure applications in e-government. The case study (qualitative research) was carried out in a company that develops Management Systems and Electronic Government, making explicit the need to adopt practices related to information security so that it adheres to the requirements of Law 13.709/2018-LGPD. Data collection took place directly in the environment in which the application of practices was observed. From this observation of security practices, a thematic model was elaborated having as axes: Technical, Cultural/Personal and Legal, then for each axis a subdivision into more specific areas was carried out, obtaining the following areas as a result: Development , Product and ICT (in

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

the Technical axis), Internal and External (in the Cultural/Personal axis) In all, 42 practices in use were identified, some of which were adopted exclusively by the advent of security with a focus on the LGPD and others already existed, being modified as necessary . Finally, all practices were described individually. In this article, the other analyzed practices were discussed and that these can contribute and help other public and private institutions in the adoption of them in the software development environment.
Keywords: e-Government, LGPD, technological management solutions, information and communication technology, information security.

1. INTRODUÇÃO

Um ambiente de desenvolvimento seguro depende entre outras coisas, que exista espaço físico e ambiente lógico adequados (ISO 15.408), que as pessoas estejam cientes da necessidade de adoção de práticas seguras e que as práticas existam e sejam constantemente verificadas. Albuquerque (2002, p. 5) em seu livro "Segurança no Desenvolvimento de Software", deixa claro que "É impossível obter um sistema seguro em um ambiente inseguro". Essa deveria de fato ser uma preocupação de toda instituição que desenvolve softwares, sejam elas públicas ou privadas, pois esse olhar garante segurança tanto a ela, quanto ao cliente, aos fornecedores e também aos colaboradores.

Para manter a segurança de informações é necessário que exista um amplo conjunto de quesitos e para Fontes (2006 p. 11), "segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.", em síntese observamos a segurança como uma série de camadas inter-relacionadas que somadas fornecem a maior segurança possível. A frequência com que esses procedimentos ocorrem varia de acordo com cada ativo de informação, alguns ocorrendo diariamente, outros com uma frequência menor.

O objetivo principal desta pesquisa foi identificar e enumerar o conjunto de medidas ou camadas de segurança da informação que foram adotadas na empresa I desenvolve Sistemas de Gestão e Governo Eletrônico em Rio do Sul-SC, visando manter a privacidade dos dados de pessoas sob sua guarda e tratamento. Esses dados foram inseridos nos sistemas de Gestão Pública de

Prefeituras, Câmaras e demais entidades municipais, pelos funcionários dessas entidades, por meio do software Atende.net operado via internet e estão sob guarda da empresa em data center privado.

Com base na definição da LGPD (Lei Geral de Proteção de Dados) em seu Artigo 5, inciso VII, a empresa enquadra-se como Operador, já que o fornecimento do produto de software de sua autoria fica condicionado a obtenção e armazenamento de dados diretamente em seu Data Center.

Para que os objetivos possam ser atingidos, este artigo está dividido em cinco partes. Iniciando por esta seção introdutória, seguindo após com a revisão da literatura, que procura descrever aspectos gerais sobre o tema central desta pesquisa: Segurança da Informação e LGPD Aplicado ao Desenvolvimento de Software. O terceiro capítulo apresenta os procedimentos metodológicos, que envolve o levantamento e observação das práticas de segurança aplicadas na empresa. Na quarta etapa são apresentados os principais resultados obtidos na adoção dessas práticas. E por fim, são apresentadas as considerações finais e as recomendações para trabalhos futuros.

2. LGPD – LEI GERAL DE PROTEÇÃO DE DADOS

De forma resumida o Legislador Brasileiro pretende com esse arcabouço legal, prevenir ataques sobre a privacidade de dados pessoais de pessoas físicas naturais ou, conforme definido na própria lei, o titular de dados.

Importante destacar que conforme a Lei, as empresas prestadoras de serviço, manutenção ou licenciamento de software possuem um papel importante e podem ser acionadas em casos que vão desde a verificação de práticas e salvaguardas dos dados sob sua posse, até a responsabilização sobre vazamentos de dados. Para tanto no Art. 50, ficam claras algumas das práticas que são esperadas dos operadores bem como de controladores.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (LGPD, 2018).

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

Yapoli em seu Blog “Desafios da LGPD em Plataformas SaaS B2B”, descreve: “Como controlador, você deve exigir práticas de privacidade e proteção de dados de seu operador, estabelecer obrigações e definir responsabilidades. Como operador, você deve estar atento às exigências tanto da lei como do controlador, para não ser eventualmente responsabilizado por danos aos titulares. O contrato de prestação de serviço, portanto, deve ser adaptado para conter disposições nesse sentido.” (YAPOLI, 2021).

O Art. 5. Da referida lei considera “tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (LGPD, 2018).

O mesmo artigo também define dado pessoal sensível como sendo: “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (LGPD, 2018).

3. SEGURANÇA DA INFORMAÇÃO

Para Fontes (2006, p. 11), “Segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.”. “A segurança da informação é aquele conceito por trás da defesa dos dados, detalhes e afins para assegurar que eles estejam acessíveis somente aos seus responsáveis de direito, ou as pessoas às quais foram enviados.” (VELOCO, 2010). Ainda, conforme Lyra (2008, p.4), “Quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente”.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

Na visão de Veloco (2010), a segurança sobre a informação existe para minimizar riscos de forma geral. Tendo a informação incorreta ou não tendo mais ela, isso pode gerar grandes problemas e muitas dores de cabeça.

> Nossa tendência natural é considerar a segurança de computadores estritamente em um contexto digital, em que computadores são acessados apenas por meio de uma rede ou de uma interface digital bem especificada e nunca são acessados diretamente ou com ferramentas físicas, como um martelo, uma chave de fenda ou um frasco de nitrogênio líquido. Entretanto, no final, a informação digital deve residir fisicamente em algum lugar, como em estados de elétrons, meio magnético ou dispositivos óticos, e acessar essa informação requer o uso de uma interface entre os mundos físico e digital. Portanto a proteção de informação digital deve incluir métodos para proteger fisicamente essa interface (GOODRICH; TAMASSIA, 2013, p. 54).

Nessa linha de pensamento, fica evidente que as ações devem ir além da segurança dos dados, é necessário ter atenção com o meio ambiente das instalações, aspectos culturais e sociais e quem tem acesso ao hardware, que está guardado a informação. As medidas tomadas com relação a segurança da informação, devem envolver ações no meio digital, físico e na cultura das pessoas envolvidas. É necessário destacar também que não haverá privacidade de dados onde não existe segurança da informação.

Segundo Albuquerque (2002, p.1) **Confidencialidade é** a “capacidade de um sistema de impedir que usuários não-autorizados vejam determinada informação, ao mesmo tempo que usuários autorizados podem acessá-la”. Observa-se na definição a preocupação em garantir o acesso a quem é devido, pois a indisponibilidade da informação é um fator prejudicial a qualquer software de computador.

Lyra (2008, p. 4) define a **Disponibilidade** como “A informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais.”. Somando-se a confidencialidade podemos dizer que a informação deve estar sim disponível, porém apenas para aqueles que realmente precisarem dela na consecução de sua atividade e ao mesmo tempo impedir o acesso de outras pessoas.

Para caracterizar **Integridade** Lyra (2008, p. 3) indica que “a informação deve estar correta, ser verdadeira e não estar corrompida”. Em outros termos não basta que a informação contenha essas características, é necessário também que outros elementos que garantam tais requisitos estejam associados a ela, acessíveis e sejam incontestáveis para todas as partes envolvidas. Soma-se aqui o não-repúdio, outra característica básica de segurança da informação.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

O **Não-Repúdio** não chega a ser uma característica tão básica quanto as anteriores, mas o não-repúdio serve para que nenhuma parte associada a informação possa contestá-la. Albuquerque (2002, p.167) define que mecanismos de não-repúdio "almejam basicamente gerar evidencias que provem que determinado usuário usou determinada função do sistema.".

Além desses fundamentos básicos a segurança da informação também se apoia em outras atividades que envolvem os seguintes assuntos ou áreas:

Na **Contratação de Pessoal** segundo ABNT (2005, p.25) os controles de segurança na contratação de pessoal têm por objetivo "Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos.".

> Convém que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação. Convém que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis. Convém que todos os funcionários, fornecedores e terceiros, usuários dos recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação (ABNT, 2005, p.25).

A **Segurança Física** segundo a ABNT (2005, p.32), "Convém que as instalações de processamento da informação crítica ou sensível sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados.".

> Os servidores de redes e demais equipamentos críticos devem estar instalados em locais protegidos contra acidentes físicos, água e sujeira, contra descargas e interrupções elétricas, contra a entrada de pessoas estranhas que não conhecem os equipamentos e outros riscos. Os ambientes em que os equipamentos ficam alocados devem possuir ventilação e se necessário, refrigeração do ar. Também devem possuir instalações elétricas adequadas e protegidas contra falhas. Os equipamentos devem estar correta e devidamente instalados (SOUSA, 2009, p. 158).

Desta forma, além de proteger os dados da organização, devemos nos preocupar bastante com as instalações físicas dos servidores, estações e da rede, pois acidentes naturais podem acontecer, sendo importante uma instalação física adequada (SOUSA, 2009).

O **Gerenciamento de Serviços Terceiros** faz-se necessário que exista um acordo com os terceiros que executam serviços dentro da empresa, pois deve existir um tempo limite e também a confiabilidade sobre os dados e as tarefas que estão sendo executadas, bem como é necessário

monitorar para garantir que o que está sendo feito pela terceirizada não vá gerar nenhum prejuízo (ABNT, 2005).

No que se refere ao gerenciamento de serviços de terceiros nas empresas, a ABNT (2005, p.42) estabelece que "Convém que a organização verifique a implementação dos acordos, monitore a conformidade com tais acordos e gerencie as mudanças para garantir que os serviços entregues atendem a todos os requisitos acordados com os terceiros.".

A **Proteção Contra Códigos Maliciosos** segundo Fontes (2006, p. 66) "Os vírus são programas que penetram no computador que utilizamos sem a nossa autorização e executam ações que não solicitamos. Normalmente, essas ações prejudicam o equipamento ou seu desempenho.".

> O vírus tem um objetivo principal: desestabilizar o sistema, seja prejudicando o seu desempenho, destruindo arquivos ou mesmo se espalhando para outros computadores. Os vírus mais comuns são os encontrados em programas e arquivos e são normalmente ativados quando o usuário acaba clicando em algum programa da Internet ou programa executável (terminação .exe). Os vírus mais prejudiciais são aqueles que tentam roubar informações sigilosas dos usuários. Estes são os chamados cavalos de troia, ou apenas trojan. Outro tipo de vírus é o *worm*, este é o mais perigoso, pois se multiplica sozinho e amplia a infecção para outros computadores através da Internet. (POZZEBOM, 2013).

"Um vírus é um pequeno programa informático, também chamado de código malicioso carregado na memória de um dispositivo e que executa as instruções que o seu autor programou.". (CCM, 2017c). Para Fontes (2006, p. 70), "A proteção contra vírus e outras pragas será efetiva se for parte de um processo de segurança da informação estruturado para a organização.".

Os ***backups*** (cópias de segurança) são os arquivamentos periódico de dados. Esse arquivamento é feito de modo que arquivos de dados possam ser restaurados caso tenham sido alterados de maneira não autorizada ou não intencional (DÂMASO, 2014). "Como os dados armazenados em computadores estão sujeitos a perdas e erros, é necessário um modo de recuperá-los no caso de falhas e protegê-los. A forma mais comum é fazer cópia dos dados e arquivos, armazenando-os em outro local, para o caso de haver perda ou alterações indevidas" (SOUSA, 2009, p. 157).

> O Backup é uma cópia de segurança. O termo em inglês é muito utilizado por empresas e pessoas que guardam documentos, imagens, vídeos e outros arquivos no computador ou na nuvem, hospedados em redes online como Dropbox e Google Drive. O objetivo da ação é o usuário se resguardar de uma ocasional perda de arquivos originais, seja por ações despropositadas do usuário como perder um CD/DVD e ter um problema com o HD, ou ainda mau funcionamento dos sistemas. Ter uma cópia de segurança permite restaurar os dados perdidos. (DÂMASO, 2014).

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

A informação pode ser alvo de ações criminosas e além disso, também é sujeita a desastres naturais. Porém independente de uma eventual perda de dados, a empresa necessita de condições e organização de recuperar informações perdidas (SOUSA, 2009).

O **Gerenciamento de Mídias Removíveis** para ABNT (2005), é necessário que haja um procedimento para tratar de mídias removíveis, da forma que garanta que os arquivos que vão ser transferidos por ali, sejam arquivos válidos e limpos. “Convém que procedimentos operacionais apropriados sejam estabelecidos para proteger documentos, mídias magnéticas de computadores (fitas, discos), dados de entrada e saída e documentação dos sistemas contra divulgação não autorizada, modificações, remoção e destruição.” (ABNT, 2005, p.50).

O **monitoramento t**em como objetivo “detectar atividades não autorizadas de processamento da informação.” (ABNT, 2005, p.60). Segundo a ABNT (2005, p.60), “Convém que as organizações estejam de acordo com todos os requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento.”.

Sobre os **controles de acesso**, Macêdo (2014) afirma que “São um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou outros programas.”. Sendo que “Uma das melhores maneiras de se defender contra-ataques é, em primeiro lugar, evitá-los. Providenciando maneiras rigorosas de determinar quem tem acesso as diversas partes de informação, muitas vezes podemos evitar ataques de confidencialidade, integridade e anonimato[...]” (GOODRICH; TAMASSIA, 2013, p. 36).

Para a (ABNT, 2005, p.65), “Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.”.

“O controle de acesso tem como função permitir o acesso do usuário a sistemas e aplicações somente se ele possuir autorização. A autorização de acesso também tem como função controlar a alçada do usuário, segmentando o que ele pode e não pode acessar.” (SOUSA, 2009, p. 154). Segundo Machado (2012a), “A restrição de acesso, embora não elimine por completo os riscos à segurança da informação, diminui em muito a ocorrência de incidentes que comprometam a continuidade das atividades do negócio.”.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

A **Política do Uso de Senhas** segundo a (ABNT, 2005, p.69), "Convém que os usuários sejam solicitados a seguir as boas práticas de segurança da informação na seleção e uso de senhas.".

> "Existem três maneiras de se garantir que um usuário é quem ele diz ser:
> 1 – Perguntar algo que só aquele usuário saberia responder corretamente;
> 2 – Solicitar a apresentação de algo que só aquele usuário teria;
> 3 – Identificar o usuário por características pessoais.
> De todas elas, a primeira alternativa é a mais fácil de ser implementada e a mais comum. A informação que somente o usuário sabe é, geralmente, uma senha individual de acesso. Apesar da simplicidade, o mecanismo possui um problema básico: a possibilidade de outra pessoa vir a saber aquele segredo." (ALBUQUERQUE, 2002, p. 129).

"As senhas foram introduzidas devido à necessidade de manter os dispositivos, dados e software de computador privados." (BEN-ITZHAK, 2014). Esta prática, "pode ser vista 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" (MACÊDO, 2014).

Uma preocupação atual sobre o tema está no fato de que a frequência da modificação de senhas poderá resultar em senhas repetidas e de baixa segurança, como a adoção de um padrão de senhas para tudo. "Os usuários tendem a memorizar chaves secretas mais fracas quando sabem que terão que mudá-las em um futuro próximo. Quando essas alterações ocorrem, eles geralmente selecionam uma chave semelhante a antiga memorizado, aplicando um conjunto de transformações comuns, como aumentar um número na senha. Essa prática fornece uma falsa sensação de segurança se qualquer um dos segredos anteriores foi comprometido, pois os invasores podem aplicar essas mesmas transformações comuns." (NIST, 2020).

O **Controle Criptográfico** de acordo com Garrett (2012), "Em linhas gerais, criptografia é o nome que se dá a técnicas que transformam informação inteligível em algo que um agente externo seja incapaz de compreender. De forma mais simples, a criptografia funciona como códigos [...]".

> A criptografia na transmissão de dados tem como objetivo codificar os dados a serem transmitidos de forma que não possam ser identificados, evitando que a informação seja capturada e entendida por estranhos. O objetivo da criptografia é transformar os dados para que não sejam entendidos por terceiros. Os dados só são reconhecidos pelo transmissor e pelo receptor que possuem a chave criptográfica, que opera como um código secreto codificando e decodificando a mensagem por meio de algoritmos, impedindo a leitura por estranhos ou pessoas não autorizadas. Vemos que esse tipo de proteção é cada vez mais importante, especialmente quando utilizamos redes públicas como a Internet, sujeita a acessos por pessoas não autorizadas. (SOUSA, 2009, p. 147).

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

Para Macêdo (2014), “A criptografia provavelmente é o aspecto mais importante da segurança de comunicações e está se tornando cada vez mais importante como um componente básico para a segurança do computador.”. Desta forma, a criptografia é “[...] uma das ferramentas principais para este fim. Para manter a confidencialidade, precisamos acima de tudo implementar ferramentas e mecanismos de proteção dos dados, como a criptografia.” (MORAES, 2015, p. 19).

Para a (ABNT, 2005, p.87) a criptografia tem por objetivo “proteger a confidencialidade, a autenticação ou a integridade das informações por meios criptográficos.”. Complementa ainda que “Convém que uma política seja desenvolvida para o uso de controles criptográficos. Convém que o gerenciamento de chaves seja implementado para apoiar o uso de técnicas criptográficas.”. (ABNT, 2005, p.87).

O protocolo HTTPS é um exemplo de implementação bem sucedida de um mecanismo de criptografia, que consiste basicamente na cifragem de dados enviados do servidor para o cliente e do cliente para o servidor, sobre o protocolo HTTP. “HTTPS (Protocolo de transferência de hipertexto seguro) é uma versão segura do protocolo HTTP que usa o SSL /TLS como protocolo para criptografia e autenticação. HTTPS é especificado pelo RFC 2818 (Maio de 2000) e usa a porta 443 por padrão em vez da porta 80” (SSL, 2021).

Sobre **vazamento de informações,** Goodrich e Tamassia (2013, p.438) afirmam que, “A política de segurança impõe restrições sobre quais ações os sujeitos em um sistema podem fazer a respeito de objetos desse sistema, a fim de atingir objetivos específicos de segurança.”. Desta forma, é necessário adotar medidas de boas práticas, instruindo os usuários a usar o computador e a rede de forma segura. Se encaixa também a questão de limitar os acessos a sites, downloads e adotar um princípio de privilégios para executar comandos e programas diversos (GOODRICH; TAMASSIA, 2013). Neste sentido, são recomendadas algumas práticas como “[...] a varredura do envio de mídia e comunicações para verificar a presença de informação oculta; o monitoramento das atividades do pessoal e do sistema, quando permitido pela legislação ou regulamentação vigente; o monitoramento do uso de recursos de sistemas de computação.” (ABNT, 2005, p.95).

O Trabalho & Segurança no Home Office teve aumento da demanda na pandemia e naturalmente é algo a ser trtado sob ótica de segurança da informação. Mesmo atuando de casa, os dados da empresa e dos clientes devem estar protegidos. Esse é o ponto: o ato de proteger as informações, mesmo estando em ambientes externos.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

> No contexto laboral e corporativo, a LGPD se aplica à toda a equipe e é necessária especial atenção quando se trabalha em home office - também chamado "trabalho remoto". Se os colaboradores manipulam as informações de suas casas (ou de outros lugares onde escolham trabalhar), as empresas não têm, a princípio, um controle tão amplo sobre a segurança existente no local onde home-office é executado, o que leva a temores pela perda ou roubo de dados. (DRUMMOND, 2020).

Mais do que nunca, justifica-se a criação de um protocolo ou medidas que possam ser trabalhadas tanto técnicas (barreiras lógicas naturais) como comportais (melhor capacitação de colaboradores para esse novo método de trabalho. “Os funcionários precisam ser treinados sobre a importância de cuidar ativamente das informações em seu poder. Isso incluiria documentação e procedimentos para quando surgir um problema e como minimizar o impacto. Pense em como seria fácil deixar um telefone celular em um ônibus e, em seguida, pense em todos os contatos que seriam armazenados apenas naquele dispositivo (talvez uma parte do banco de dados da empresa).” (DRUMMOND, 2020).

O **OWASP (Open Web Application Security Project),** ou Projeto Aberto de Segurança em Aplicações Web, trata-se de uma comunidade que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web.

> The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web. (OWASP, 2021).

Todo o material criado é gratuito e aberto, podendo ser simplesmente seguido conforme descrito, modificado ou mesclado com outros materiais conforme conveniência de cada entidade ou empresa.

“**Security-by-Design** é uma abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas. Isso inclui a incorporação de especificações de segurança no projeto, avaliação de segurança contínua em cada fase e adesão às melhores práticas” (CSA, 2017).

O objetivo principal do princípio é a adoção de práticas de segurança, antes, durante e depois do desenvolvimento de um software. Em termos práticas pode-se dizer que não é possível implementar segurança em um software posterior a sua construção, por meio de recursos isolados,

afinal segurança deve ser tratada como requisito não funcional de qualidade de software, um conceito, e não uma *Feature* do sistema.

Nesse sentido, existem diversas normas e guias que podem ser utilizados para obtenção desses requisitos. É necessário portanto, que a especificação de "segurança do software inicie na fase de análise, gerando um documento de especificação de segurança do sistema usando a ISO/IEC 15.408 como um guia." (ALBUQUERQUE, 2002).

"O significado de **PRIVACY BY DESIGN** é um conceito de privacidade talvez seja melhor expressa como "autodeterminação informativa", um termo usado pela primeira vez em uma decisão constitucional alemã sobre informações pessoais coletados durante o censo de 1983 da Alemanha." (CAVOUKIAN, 2013).

Trata-se de uma metodologia criada pela Dra. Ann Cavoukian que tem como objetivo manter a privacidade de informações pessoais coletadas por empresas.

"Assim como a segurança, a privacidade não precisa diminuir a funcionalidade da tecnologia. Uma vez devidamente compreendida e implementada, a privacidade funciona em conjunto com a tecnologia e aprimora sua funcionalidade na medida que aumenta a satisfação e confiança do usuário final. A tecnologia não é prejudicada pela privacidade, mas, ao contrário, torna-a muito melhor." (CAVOUKIAN, 2013).

A metodologia é composta por sete fundamentos que são essenciais, sendo eles os principais fundamentos do Privacy by Design:

- Ser proativo e não reativo: Proteção antes do fato e não depois;
- A privacidade e a proteção do usuário devem ser garantidas sempre: O usuário não precisa agir para estar seguro;
- Incorporar a privacidade ao projeto: não sendo apenas um adendo, mas sim parte do que será desenvolvido;

- Todas as possíveis funcionalidades devem ser completas e protegidas, gerando um benefício mútuo, para o usuário e para a empresa;

- A segurança deve estar presente desde a captação até a destruição ou compartilhamento do dado, ou seja, de ponta a ponta;

- Manter a transparência com o titular dos dados: informar sobre o motivo de coleta das informações e quem possui acesso à elas;

- A privacidade do usuário deve ser respeitada sempre;

O **Privacy By Design e o Privacy By Default**, são metodologias semelhantes e na verdade complementares, pois um bom projeto de software que proveja segurança em todo seu ciclo de desenvolvimento, gerará em tese, um produto de software seguro, porém o uso dos recursos de segurança não devem ser opcionais tampouco de preferência do usuário.

"Sendo assim, os projetos gerados através deste conceito são proativos e oferecem controle para que o usuário altere configurações padrão do sistema, optando por fornecer os dados ou não, e utilizar o produto ou serviço livremente. Agora, quando falamos nesta segunda metodologia, é preciso entender que ele significa que assim que o produto ou serviço é lançado ao público, as configurações mais seguras são aplicadas por padrão." (ZEFERINO, 2020).

4. METODOLOGIA E ANALISE DAS PRÁTICAS OBSERVADAS

A metodologia utilizada no desenvolvimento do trabalho fora organizada em duas etapas, sendo a primeira, de caráter exploratório, onde foram levantados os temas relevantes sobre segurança da informação, manutenção da privacidade de dados e LGPD, a partir da revisão da literatura. Na segunda etapa, utilizando a o método qualitativo, por meio de estudo de caso, teve como objetivo levantar e documentar as práticas adotadas na empresa, por meio observação onde o pesquisador pode ser definido como um participante completo, por fazer parte do quadro de empregados da empresa.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

Richardson (1999, p.79) diz que, "O método qualitativo difere em princípio, do quantitativo à medida que não emprega um instrumental estatístico como base do processo de análise de um problema. Não pretende numerar ou medir unidades ou categorias homogêneas.". O autor ainda afirma que "[...] o método quantitativo representa, em princípio, a intenção de garantir a precisão dos resultados, evitar distorções de análise e interpretação, possibilitando, consequentemente, uma margem de segurança quanto às inferências." (RICHARDSON, 1999, p. 70).

Segundo Gil (2017), o estudo de caso, consiste no estudo profundo e exaustivo de um ou poucos casos, de maneira que permita seu amplo e detalhado conhecimento.

As práticas aqui descritas foram classificadas em três grupos distintos: Técnico (aquelas aplicadas com enfoque na tecnologia especialmente), as Culturais ou Pessoais (práticas focadas nas pessoas sejam colaboradores da empresa ou usuários do sistema) e Jurídicas (atividades visando levantamento e entendimento de questões jurídicas). Adicionalmente cada grande eixo foi subdividido em áreas mais específicas, sendo que cada eixo e cada área foram identificados com uma letra correspondente.

Foram identificadas ao todo 42 práticas principais e para facilitar o entendimento essa estrutura é demonstrada a seguir no Quadro 1 - Distribuição Temática das Práticas.

Quadro 1 - Distribuição Temática das Práticas

Eixo	Técnico (T)			Cultural/Pessoal (C)		Jurídico (J)
Área	Desenvolvimento (D)	Produto (P)	TIC (T)	Interno (I)	Externo (E)	
Ações	(TD1) Auditoria de Código Externo	(TP1) Adoção do Privacy by Default	(TT1) Elaboração e Publicação do PSI e Documentos Derivados	(CI1) Ações de Capacitação de Pessoal	(CE1) Foco na Prevenção de Incidentes	(J1) Revisar regulamentos e Leis
	(TD2) Adoção do Security By Design	(TP2) Proatividade no Monitoramento Data Center	(TT2) Segmentação de Redes	(CI2) Campanhas de Conscientização Internas	(CE2) Por que se preocupar com segurança?	(J2) Elaborar documentos: Termos de uso, Política de Privacidade, Política de Cookies, etc.
	(TD3) Controle de Chaves de Criptografia	(TP3) Política de Acesso usuário Normal x Técnico	(TT3) Acesso Físico e Lógico controlados	(CI3) Implantação de Cultura proativa de Segurança	(CE3) Comunicação direta LGPD – Somos operadores	(J3) Criar e manter canal de comunicação exclusivo LGPD.
	(TD4) Repositórios	(TP4)	(TT4)	(CI4)	(CE4) Necessidade	(J4) Elaboração

	Internos Apenas	Mapeamento de Tratamentos de Dados Pessoais	Mapeamento de ações: Antes, Durante e Depois de Incidentes	Modificações no Manual do Colaborador	de Backup e Gestão Local do Cliente	de Termo de Responsabilidade e do Colaborador
	(TD5) Adoção de Padrões de Segurança (OWASP)	(TP5) Matriz de Tratamentos de Dados x Dados Pessoais	(TT5) Infraestrutura de backup	(CI5) Anonimização de Dados Pessoais em Demonstrações		(J5) Auxilio na elaboração de Decretos e Leis municipais sobre o tema.
	(TD6) Equipe White Hat - *White Box.*	(TP6) Teste Constante de Backups de Clientes	(TT6) Monitoração de Ativos de Informação			
	(TD7) Validação da Entrada de Dados (Front-End e Back-End)	(TP7) Auditoria e Mecanismos de Não Repúdio	(TT7) Automação do Restore de Backups de clientes com anonimização de dados			
	(TD8) Framework vs Segurança	(TP8) Equipe White Hat - *Black Box.*	(TT8) Adoção de Política de Segurança na contratação de Terceiros			
	(TD9) Rastreabilidade Completa de Artefatos	(TP9) Aumento do nível de criptografia TLS.	(TT9) Restrição de Acesso e Uso de Mídias Removíveis			
	(TD10) Anonimização de Dados					

Fonte: Acervo dos Autores

No primeiro artigo sobre LGPD em 2022 foram abordadas as 22 primeiras e nesse segundo artigo por questões relacionadas ao tamanho máximo de páginas, disponíveis em <http://reis.unisociesc.com.br/index.php/reis/article/view/332/317>. Algumas técnicas, ferramentas e suas versões, bem como o método exato de como elas são aplicadas, foram intencionalmente suprimidas.

5. RESULTADOS E DISCUSSÕES

J1 - REVISAR REGULAMENTOS E LEIS

Assim que a LGPD foi promulgada, um conjunto enorme de entidades, pessoas e empresas, se apresentaram como “especialistas no assunto”. A empresa fez sua “lição de casa” ao buscar conhecimento sobre o tema, inicialmente pela própria equipe técnica interna. Mas com o passar do tempo percebeu-se a necessidade de pessoas especializadas com foco na LGPD.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

Diante disso, dois advogados foram contratados como empregados (em tempo integral) e logo iniciaram uma revisão completa dos regulamentos e leis, não só a LGPD, mas preceitos da própria RGPD e outras interligadas como a Lei de Acesso a Informação e Lei da Transparência.

Essa ação foi extremamente importante, pois deu a equipe técnica o apoio necessário no melhor entendimento das ações a serem realizadas.

J2 - ELABORAR DOCUMENTOS: TERMOS DE USO, POLÍTICA DE PRIVACIDADE, POLÍTICA DE COOKIES, ETC.

Como consequência da contratação de equipe jurídica focada no aparato legal, um conjunto de documentos foi criado, com vistas a N004 – Norma de Segurança de Produtos, concretizando uma diretriz do PSI.

Alguns dos documentos elaborados incluem uma Política de Privacidade por Produto de Software, o Termo de Uso do software, Política de Uso Aceitável do produto, Política de Cookies, Termos de Consentimento do usuário final para recebimento de notificações internas no software relacionados a marketing e outros documentos internos. Os documentos estão acessíveis e públicos, podendo ser consultados por qualquer pessoa nos seguintes endereços:

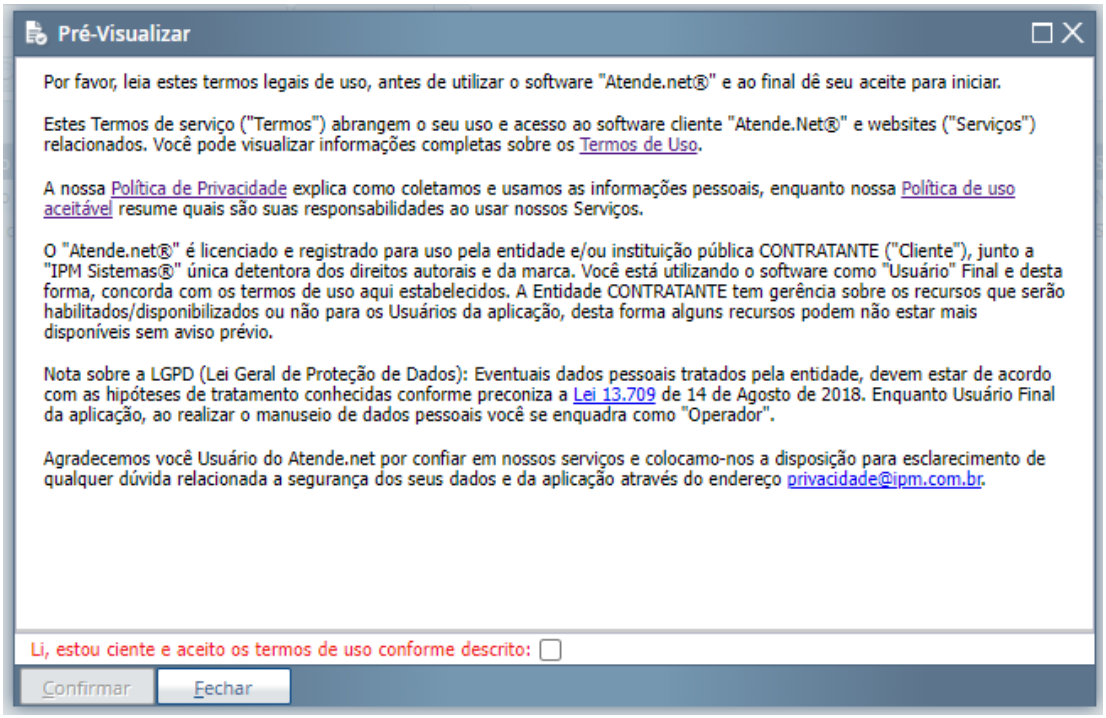
- Termos de Uso: https://news.atende.net/docs/nws_termos_de_uso_atende.html
- Política de Uso Aceitável: https://news.atende.net/docs/nws_politica_de_uso_aceitavel_atende.html;
- Política de Privacidade: https://news.atende.net/docs/nws_politica_privacidade_atende.html;
- Política de Uso de Cookies: https://news.atende.net/docs/nws_politica_de_uso_de_cookie.html;

Importante destacar sobre a necessidade de revisão e atualização constante desses documentos. Embora essa seja uma atividade necessária deve-se ter em mente que os usuários devem ser notificados quando ocorrerem. Para isso é necessário no entanto que o usuário se identifique de algum modo para que seja notificado posteriormente.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432
Compartilhar conhecimento é conhecer o mundo.
unisociesc

Os usuários internos do sistema ao realizarem o primeiro acesso são informados sobre os termos de uso e devem fazer o aceite formal deles para que possam continuar operando, podendo ser visto na Figura 6:

Figura 1 - Termos de Uso do Usuário do Sistema



J3 - CRIAR E MANTER CANAL DE COMUNICAÇÃO EXCLUSIVO LGPD

Como forma de atendimento ao que define a LGPD, fora criado um canal de comunicação exclusivo para questões envolvendo privacidade de dados pessoais. Esse canal consiste em um endereço de e-mail privacidade@ipm.com.br, acessível diretamente pelas políticas e termos de uso do software e as demandas são direcionadas a mesma equipe jurídica que trata dos assuntos relacionados a LGPD.

Como as requisições podem requerer dados que são de propriedade do cliente, elas são avaliadas e caso necessário, são encaminhadas diretamente ao cliente que recebe suporte jurídico no atendimento da demanda.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

Importante destacar que cada cliente pode (e deve) disponibilizar seu próprio canal de recebimento de demandas relacionadas a LGPD, sendo que para isso existe um serviço no Portal do Cidadão/Autoatendimento disponível aos titulares de dados, onde a demanda deve ser gerenciada e respondida por rotina interna do sistema, pelo Encarregado de Tratamento de Dados.

J4 - ELABORAÇÃO DE TERMO DE RESPONSABILIDADE DO COLABORADOR

O Termo de responsabilidade é um documento previsto no manual do colaborador que é assinado por cada empregado da empresa. Ele é constituído de um conjunto de deveres dele perante a empresa e seus clientes. O termo de responsabilidade já existia antes da adoção dessa ação, mas a partir dela ele foi reformulado, buscando melhor enquadramento perante as condições legais atuais.

É importante que os colaboradores tenham ciência e efetivamente participação no cumprimento das diretrizes de segurança da informação. Além disso, alguns dos editais de contratação de software que a empresa participa, exigem tal formalidade.

J5 - AUXILIO NA ELABORAÇÃO DE DECRETOS E LEIS MUNICIPAIS SOBRE O TEMA.

Como forma de auxiliar seus clientes (que são entidades públicas municipais) a empresa disponibilizou expertise jurídico para dar suporte as ações a serem implementadas por eles. Com isso uma das ações realizadas foi a criação do documento em formato de Nota Técnica, NT 224/2020 – Conformidade com a LGPD, conforme previsto pela PSI:

> "No atual cenário de Segurança da Informação e Privacidade de dados, há de se mencionar também a LGPD (Lei Geral de Proteção de Dados) que deixa claro a necessidade e obrigatoriedade de se manter a constante vigilância sobre a privacidade de dados de pessoas naturais. Neste aspecto e pelo fato de a IPM Sistemas fornecer software como serviço (SaaS), estamos enquadrados como Operadores. Mais informações podem ser obtidas na NT 224/2020 – Conformidade com a LGPD e na Cartilha disponibilizada sobre a LGPD – Disponível em (Dicionário) Repositório Central > Documento(s) > Outros Documentos > Segurança Institucional > Cartilha - LGPD (PDF)" (IPM Sistemas – PSI, 2020, p. 3).

Em sequencia o grupo jurídico preparou documentos e minutas que auxiliam os clientes tanto na identificação do Encarregado de Dados, como nas formalidades necessárias para nomeá-lo. Também foram elaboradas minutas com objetivo de permitir elaborar Decreto e/ou Lei regulamentando ações de Governo Digital, conforme previsto na Lei 14.129/2021, como o uso de Assinaturas Eletrônicas Avançadas.

Revista de Extensão e Iniciação Científica da UNISOCIESC
REIS ISSN 2358-4432

6. CONSIDERAÇÕES FINAIS

O presente artigo buscou realizar um levantamento de bases teóricas abordadas na revisão de literatura e que estejam relacionados a adoção de práticas de segurança em ambientes de desenvolvimento de software. O estudo de caso foi efetuado na empresa IPM Sistemas Ltda por meio da descoberta e observação das práticas de segurança em uso.

Para alcançar o objetivo principal desta pesquisa, que foi descrever um conjunto de práticas de segurança da informação adotadas pela empresa, com foco no provimento da privacidade de dados pessoais, foi realizado um levantamento por meio de observação com base na revisão de literatura, formando a base para o estudo de caso. Como resultado as práticas observadas foram classificadas em três grandes grupos, subdivididos em 5 sub-grupos culminando num total de 42 práticas relevantes à segurança da informação, sendo possível então realizar a descrição individual delas.

Com a descrição dessas práticas realizou-se a análise delas com base na revisão de literatura. Nas práticas observadas e descritas, foram apontados também meios e mecanismos para adoção delas, podendo ser utilizados e adaptados para a realidade de outras empresas.

De maneira geral as práticas evidenciadas são tratadas com bastante relevância no ambiente de desenvolvimento de softwares, de uma forma natural e habitual, ou seja, fazem parte da cultura da empresa. É necessário, porém que esse conjunto de práticas seja realimentado, com base na observação e auditoria constante, utilizando ferramentas mais adequadas, eficientes, com custo benefício apropriado, com foco na manutenção da segurança e consequente privacidade das informações pessoais sob guarda da empresa.

Por fim, entre os temas sobre segurança das informações abordadas na pesquisa e com base nas observações realizadas, é importante que a empresa possa também em médio/longo prazo estabelecer metas para aplicar outras práticas ou melhorar as já existentes, com objetivo de aderir a

algum padrão ou norma já constituída no mercado o que poderá melhorar ainda mais para a imagem da mesma perante a sociedade..

REFERÊNCIAS

ALEXANDRINI, Fábio, NARDELlI, Cleber, PRIMEIRA FASE DA SEGURANÇA DA INFORMAÇÃO E LGPD APLICADO NO DESENVOLVIMENTO DE SOFTWARE GOVERNO ELETRÔNICO, Revista Reis, v. 9 n. 1 (2022): REIS - 2022 - N1 / Janeiro – Junho/2022, disponível em <http://reis.unisociesc.com.br/index.php/reis/article/view/332/317> Acesso em: 04/06/2023.

ALBUQUERQUE, Ricardo. **Segurança no Desenvolvimento de Software**: como garantir a segurança do sistema para seu cliente usando a ISO/IEC. Rio de Janeiro: Campus, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002: 2005**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. ABNT, 2005.

BEN-ITZHAK, Yuval. **O futuro das tecnologias de autenticação do consumidor.** 2014. Disponível em <https://blog.winco.com.br/o-futuro-das-tecnologias-de-autenticacao-do-consumidor>. Acesso em: 25/09/2021.

CCM. **Banco de dados.** 2017a. Disponível em <https://br.ccm.net/contents/65-bancos-de-dados>. Acesso em: 22/09/2021.

CCM. **Vírus de computador.** 2017c. Disponível em <https://br.ccm.net/faq/46464-saiba-como-detectar-um-malware-e-se-proteger>. Acesso em: 24/09/2021.

CAVOUKIAN, Ann, Ph.D., DIXON, Mark. **Privacy and Security by Design**: An Enterprise Architecture Approach. 2013. Disponível em < https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf >. Acesso em: 30/09/2021.

DÂMASO, Lívia. **O que é backup e como fazer?** 2014. Disponível em < https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/08/o-que-e-e-como-fazer-backup.html>. Acesso em: 22/09/2021.

DRUMOND, Marcílio Guedes. **Segurança da Informação e Proteção de Dados no Home Office**. Disponível em < https://www.migalhas.com.br/depeso/319235/seguranca-da-informacao-e-protecao-de-dados-no-home-office >. Acesso em 03/10/2021.

FONTES, E. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

GARRETT, Filipe. **O que é criptografia?** 2012. Disponível em < https://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html>. Acesso em: 26/09/2021.

GOODRICH, Michael T; TAMASSIA, Roberto. **Introdução à segurança de computadores**. Porto Alegre: Bookman, 2013.

IPM Sistemas. **PSI - Política de Segurança da Informação**: Documento interno da empresa, disponível nos repositórios internos. IPM Sistemas, 2020.

LGPD, **Lei Geral de Proteção de Dados**. 2018. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 26/09/2021.

LYRA, Mauricio Rocha. **Segurança e Auditoria em Sistemas de Informação**. 2008. Rio de Janeiro: Editora Ciência Moderna.

MACÊDO, Diego. **Modelos e mecanismos de segurança da informação**. 2014. Disponível em <https://www.diegomacedo.com.br/modelos-e-mecanismos-de-seguranca-da-informacao>. Acesso em: 20/09/2021.

MACHADO, Marcel Jacques. **Controle de acessos.** 2012a. Disponível em <https://marceljm.com/seguranca-da-informacao/controle-de-acessos>. Acesso em: 22/09/2021.

MORAES, A. F. de. **Firewalls**: segurança no controle de acesso. São Paulo: Érica, 2015.

NIST. **Special Publication 800-63: Digital Identify Guidelines**. 2020. Disponível em < https://pages.nist.gov/800-63-FAQ/#q-b05 >. Acesso em: 03/10/2021.

OWASP. **Open Web Application Security Project**. 2021. Disponível em < https://owasp.org/ >

POZZEBOM, Rafaela. **O que é vírus de computador?** Disponível em <https://www.oficinadanet.com.br/seguranca/27318-o-que-e-um-virus-de-computador>. Acesso em: 20/09/2021.

RICHARDSON, R. J. **Pesquisa social:** métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

SOUSA, Lindeberg Barros de. **Redes de computadores**: guia total. São Paulo, Érica, 2009.

SSL. **O que é HTTPS?** 2021. Disponível em <https://www.ssl.com/pt/faqs/o-que-%C3%A9-https/>. Acesso em 24/10/2021.

VELOCO, Thássius. **O que é segurança da informação?** 2010. Disponível em <https://tecnoblog.net/43829/o-que-e-seguranca-da-informacao/>. Acesso em: 20/09/2021.

YAPOLI. **Desafios da LGPD em plataformas SaaS B2B**. Disponível em <https://yapoli.com/blog/pt/desafios-da-lgpd-em-plataformas-saas-b2b-parte-3>. Acesso em: 26/09/2021.

YIN, Robert K. **Estudo de caso:** planejamento e métodos. Porto Alegre: Bookman, 2015.

ZEFERINO, Denis. **Conceito de Privacy by Design e sua relação com a LGPD**. 2020. Disponível em < https://www.certifiquei.com.br/privacy-by-design/ >. Acesso em: 30/09/2021.