SEGURANÇA DA INFORMAÇÃO E LGPD APLICADO NO DESENVOLVIMENTO DE SOFTWARE

Cleber Nardelli[1]

[1]Coordenador de Pesquisa & Desenvolvimento – IPM Sistemas Ltda
Rio do Sul – SC – Brasil
[1]Docente do Centro Universitário para Desenvolvimento do Alto Vale do Itajaí - UNIDAVI

clebernardelli@gmail.com

ABSTRACT
This article aims to describe 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. For a better understanding of the context, a literary review was carried out. Based on the observation of security practices, a thematic model was developed having as axes: Technical, Cultural/Personal and Legal, subdivided into the following areas: Development, Product and ICT (in the Technical axis), Internal and External (in the Cultural/ Folks). The Legal axis was not subdivided. 42 practices were identified, some of which were adopted exclusively for security with a focus on the LGPD and others already existed, being modified as necessary. Finally, a summary of the best practices was drawn up.

Keywords: software development, information security, LGPD.

RESUMO
Este artigo tem como principal objetivo descrever 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. Para um melhor entendimento sobre o contexto, uma revisão literária foi realizada. A partir da observação das práticas de segurança, um modelo temático foi elaborado tendo como eixos: Técnico, Cultural/Pessoal e Jurídico, subdivididos nas seguintes áreas: Desenvolvimento, Produto e TIC (no eixo Técnico), Interno e Externo (no eixo Cultural/Pessoal). O eixo Jurídico não foi subdividido. Foram identificadas 42 práticas, sendo algumas adotadas exclusivamente para segurança com foco na LGPD e outras já existiam, sendo modificadas como necessário. Por fim, um resumo das melhores práticas fora elaborado.

Palavras-Chave: desenvolvimento de software, segurança da informação, LGPD.

1 INTRODUÇÃO

Um ambiente de desenvolvimento seguro depende, entre outras coisas, que exista espaço físico e ambiente lógico adequados ISO 15.408 (2009), 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.

Em 2015 a IPM Sistemas Ltda formalizou o comitê interno de segurança da informação e em seguida, fora elaborado o PSI (Política de Segurança da Informação). Um conjunto de atividades vem sendo conduzido na empresa desde então, como participação em eventos ligados ao tema, treinamentos internos para desenvolvedores, projetistas, testers e consultores técnicos, repasse de conhecimento a membros externos e clientes, entre outros.

Em 2018 com a promulgação da LGPD e pelo fato de a empresa enquadrar-se como operador perante a mesma, observou-se a necessidade de alcançar maior aderência, sendo uma das primeiras ações neste foco a contratação de advogado, sua capacitação e inclusão na equipe técnica. Hoje essa equipe jurídica já conta com três pessoas com dedicação exclusiva que auxiliam pessoal da área de negócio e clientes.

O objetivo principal desta pesquisa é identificar e enumerar o conjunto de medidas ou camadas de segurança da informação que foi adotado na empresa 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 IPM Sistemas Ltda 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 1, introdutória, seguindo após para a Seção 2, 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. A sessão 3 apresenta os procedimentos metodológicos, que envolve o levantamento e observação das práticas de segurança aplicadas na empresa. Já na Sessão 4 são apresentados os principais resultados obtidos na adoção dessas práticas. E por fim, na sessão 5, são apresentadas as considerações finais.

2 REVISÃO DA LITERATURA

2.1 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.

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).

2.2 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".

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 (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 guardando a informação.

3 METODOLOGIA

3.1 MÉTODO DE PESQUISA

A metodologia utilizada no desenvolvimento do trabalho foi 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. A segunda etapa, utilizando o método qualitativo, por meio de estudo de caso, teve como objetivo levantar e documentar as práticas adotadas na empresa, por meio de observação onde o pesquisador pode ser definido como um participante completo, por fazer parte do quadro de empregados da empresa.

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.

4 ANALISE DAS PRÁTICAS OBSERVADAS

O estudo em questão descreve diversas ações que foram levantadas e discutidas internamente, sendo em seguida implementadas no centro de tecnologia da IPM Sistemas Ltda, em Rio do Sul, SC. Algumas dessas práticas já existiam e outras são totalmente novas. Não se procurou aqui esgotar o tema, sendo apenas descritas resumidamente as práticas observadas.

Após levantadas e discutidas, procurando uma melhor organização, elas foram então classificadas em três grupos distintos, sendo: 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. Essa estrutura é demonstrada a seguir na Tabela 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	(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 e Políticas
	(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 Internos Apenas	(TP4) Mapeamento de Tratamentos de Dados	(TT4) Mapeamento de ações: Antes, Durante e Depois de	(CI4) Modificações no Manual do Colaborador	(CE4) Necessidade de Backup e Gestão Local do Cliente	(J4) Elaboração de Termo de Responsabilidade do

		Pessoais	Incidentes			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					

Tabela 1 - Distribuição Temática das Práticas

Buscando melhorar ainda mais na identificação de cada prática observada, elas foram codificadas e sequenciadas cada uma em seu eixo/área.

Embora todas as práticas observadas estejam presentes na Tabela 1, por conta da limitação de espaço do presente artigo, procurou-se apresentar destacado na cor laranja uma amostra de apenas 11 delas descritas a seguir de forma sucinta. Essa seleção levou em consideração fatores ligados a engenharia de software e relação direta com a LGPD. Algumas técnicas, ferramentas e suas versões, bem como o método exato de como elas são aplicadas, foram intencionalmente suprimidas.

4.1 TD1 – AUDITORIA DE CÓDIGO EXTERNO

Para esta e outras práticas a seguir descritas, o PSI (Política de Segurança da Informação) da empresa define algumas diretrizes. Neste caso a política estabelece a necessidade da elaboração de um documento denominado P033 – Padrão de Segurança de Aplicações.

Dentre as práticas descritas, todo código/biblioteca/funcionalidade que é obtido por meio de uma fonte externa como Stackoverflow ou GitHub, deve ser auditado previamente antes de ser incorporado como recurso do sistema. A auditoria é realizada por meio de revisão de código conduzida por um membro do comitê interno de segurança, podendo este solicitar auxilio de outras pessoas, normalmente da equipe de P&D. Além da auditoria também existe o registro formal do uso da fonte externa realizado pelo próprio programador na ferramenta interna de trabalho.

Importante destacar, no entanto, que pequenos trechos de código podem ser transcritos ou copiados de fontes externas, sem necessitar dessa auditoria.

Sobre isso vale citar a definição do próprio PSI quanto ao que é considerado um ambiente de desenvolvimento seguro, onde no item 5 descreve: “Restrição de acesso à internet em ambientes de desenvolvimento – É muito fácil incorporar na aplicação um trecho de código ou uma biblioteca inteira totalmente insegura. Isso permite, por exemplo, que dados sejam vazados”. IPM Sistemas (2020, p. 15).

4.2 TD4 - REPOSITÓRIOS INTERNOS APENAS

Não é permitido o uso de repositórios externos ou públicos. Todos os artefatos (arquivos de projeto ou arquivos de código fonte) são armazenados em repositórios mantidos em servidores internos da empresa, com isso diminui-se consideravelmente a possibilidade de inclusão de trechos de códigos maliciosos no sistema, bem como melhora a própria proteção de direitos intelectuais e de propriedade sobre os artefatos produzidos.

4.3 TD5 - ADOÇÃO DE PADRÕES DE SEGURANÇA (OWASP)

A adoção de procedimentos de segurança conforme algum guia ou orientação previamente estabelecido auxilia bastante na assertividade das ações. Os mecanismos de verificação como os listados a seguir, adicionam uma camada de segurança importantíssima na aplicação.

Embora extensa, essa lista não abrange todas as práticas adotadas na empresa.

- Não utilizar comandos do sistema operacional na programação de qualquer funcionalidade e validar se nos dados de entrada existem potenciais comandos do SO;
- Requerer autenticação para todas as páginas e recursos, exceto para aqueles que são intencionalmente públicos;
- Os controles de autenticação são executados apenas em um sistema confiável, neste caso do cliente o conteúdo que é enviado ao servidor é apenas um hash da senha do usuário, e o restante da lógica deve estar no lado servidor;
- Toda tentativa de autenticação, bem ou mal sucedida, é armazenada no servidor e na próxima autenticação bem sucedida o usuário deve ser alertado exibindo para ele um histórico de tentativas de acesso anteriores;
- Nenhum técnico de manutenção deve ter acesso a qualquer senha de qualquer usuário do sistema, nem mesmo ao recuperar senhas perdidas, redefinir novas senhas ou criar usuários;
- Ao ocorrer alguma falha de autenticação, apenas deve ser informado ao usuário que houve “Falha de Autenticação”, sem nenhuma informação adicional, como “Usuário não encontrado” ou “Senha Inválida”;
- Desativar a conta do usuário após 3 tentativas de login mal sucedidas. Isso não é opcional e está em acordo com o Privacy By Default;
- A senha dos usuários deve ter alto nível de segurança, exigindo-se a redefinição a cada 90 dias e observados os critérios de tamanho, caracteres e blacklist de senhas;

- Nas migrações e implantações do sistema, mesmo que as contas de usuários sejam migradas, todas as senhas devem ser refeitas no primeiro acesso e um e-mail contendo uma senha aleatória deve ser enviada ao usuário;
- Obrigatoriamente todos os dados trafegados devem estar em um canal confiável, utilizando-se de protocolo HTTPS com algoritmo de verificação seguro, como TLS 1.2 ou superior;
- A aplicação deve validar o domínio e o caminho para os cookies de sessão autenticados;
- Apenas domínios previamente conhecidos e validados no servidor devem ser aceitos nas requisições;
- Definido e configurado o atributo "secure" para cookies transmitidos através de uma conexão TLS;

4.4 TD6 – EQUIPE WHITEHAT – WHITE BOX

As empresas têm investido cada vez mais na adoção de equipes de segurança em diferentes níveis. A equipe de segurança que procura auditar, identificar ou interceptar possíveis vulnerabilidades em software é chamada de white hat.

Trata-se de um profissional que terá as características de um hacker e as utilizará para combater possíveis ataques, pautando seu trabalho com ética e segurança.

A nível de desenvolvimento, a equipe que atua nessa função é denominada de white box ou caixa branca, justamente por que eles possuem acesso aos códigos fonte. O objetivo é analisar o sistema internamente buscando por vulnerabilidades por meio da revisão de código fonte do sistema.

Observa-se aqui que a equipe de white box realiza também ações de capacitação junto aos programadores e analistas de sistemas, orientando os esforços na melhoria de segurança no ambiente de desenvolvimento.

4.5 TD9 - RASTREABILIDADE COMPLETA DE ARTEFATOS

Esse recurso é o resultado de diversas práticas de Engenharia de Software. Normalmente, no desenvolvimento de aplicações diversas ferramentas de produtividade são utilizadas para as mais diversas finalidades como (1) gerenciamento de demandas, (2) engenharia de requisitos, (3) controle de versão de código fonte e outros artefatos/repositórios, (4) ferramenta para bugtracker, (4) gerenciamento e automação de testes, (5) ferramenta para gerenciar e realizar deploy/atualização da aplicação, (6) gerenciamento da central de atendimento, entre outros.

Normalmente essas ferramentas estão dissociadas, poucas se comunicam e muitas vezes essa integração não é configurada. Como prática recomendada observada na empresa, verifica-se a existência de uma ferramenta interna, de produção/manutenção própria para gerenciamento de todo o ciclo de vida do desenvolvimento de software, o que (neste caso) garante uma completa rastreabilidade de todos os artefatos envolvidos.

Um exemplo disso é a rastreabilidade entre Requisitos x Classes de código fonte x Tabelas do Banco de dados x Bugs x Cenários de Teste. Uma vez que uma vulnerabilidade foi identificada, um cenário de teste é mapeado e um bug de segurança descrito, sendo o bug relacionado ao cenário de teste e esse ao requisito que implementa aquela funcionalidade.

4.6 TP1 - ADOÇÃO DO PRIVACY BY DEFAULT

O conceito de Privacy By Default deve ser aplicado ao produto de software em execução de tal modo que tanto o usuário como o administrador local não precisem definir as configurações de segurança.

De acordo com o PSI (Política de Segurança da Informação) da empresa, esta definição de medidas de segurança aplicadas especialmente nos produtos deve ser norteada da seguinte forma:

> "O Comitê de Segurança Interno, deverá elaborar o documento N004 - Norma de Segurança de Produtos, sendo este um instrumento para descrever em termos gerais todas as regras de segurança que qualquer produto de software desenvolvido pela IPM Sistemas deve adotar, incluindo as mencionadas acima. As regras definidas também devem nortear o processo de desenvolvimento de aplicações." IPM Sistemas (2020, p. 21).

Sobre isso, uma medida que fora adotada pela empresa foi a criação de um conceito interno de políticas de segurança aplicadas no software, em três níveis diferentes, sendo básico, intermediário e forte. O padrão aplicado em todos os clientes é forte e este não pode ser alterado por nenhum técnico da empresa, administrador local do cliente ou usuário da aplicação.

4.7 TP4 - MAPEAMENTO DE TRATAMENTOS DE DADOS PESSOAIS

Seguindo instruções disponibilizadas pelo Governo Federal, por meio do Guia de Elaboração de Inventário de Dados Pessoais[1], realizou-se também a atividade de inventário de tratamentos de dados pessoais, realizados durante a execução do(s) sistema(s). Nessa ação o foco era encontrar tratamentos de dados e dados pessoais (sensíveis ou não), tratados pelo produto.

Para isso cada área de aplicação fez uma busca nas rotinas sob sua responsabilidade, procurando identificar o propósito ou finalidade, duração, ciclo de vida, métodos de segurança exclusivos para o tratamento, dados pessoais envolvidos, hipóteses legais onde o tratamento é aplicado e dispositivos legais que amparam o uso do tratamento.

Como resultado, foram identificados 98 tratamentos, contendo um total de 89 dados pessoais específicos e diferentes. Os dados pessoais foram catalogados por categorias, conforme orientações do guia, sendo identificadas 64 categorias diferentes. Uma categoria de dados em especial trata daqueles denominados sensíveis.

4.8 TP5 - MATRIZ DE TRATAMENTOS DE DADOS X DADOS PESSOAIS

A partir do levantamento realizado na ação TP4, foi possível identificar de forma clara quais são os dados pessoais tratados no software e fazer uma matriz cruzando-os com os seus respectivos tratamentos e por meio de quais funcionalidades são realizados. Além

[1] Guia disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf.

disso, também se identificou quais os databases e tabelas onde esses dados são armazenados.

Em seguida, ações de proteção a esses dados foram aplicadas em áreas diferentes, incluindo o desenvolvimento de software, como criptografia de dados sensíveis, validação de dados com foco especial nas rotinas envolvidas, anonimização de dados apresentados de forma aberta (sem depender de login e privilégios de acesso), etc.

4.9 TT1 - ELABORAÇÃO E PUBLICAÇÃO DO PSI E DOCUMENTOS

O PSI (Política de Segurança da Informação) é um documento extremamente importante pois indica a toda organização quais são as diretrizes da empresa, em se tratando exclusivamente de Segurança da Informação.

A elaboração e publicação desse documento foi importantíssima, pois a partir dele diversos outros guias, normas e documentos foram criados.

Importante destacar que por meio da elaboração e publicação do PSI, a alta direção da empresa dá poderes importantes para outras áreas estratégicas e que essas possam executar as ações necessárias.

4.10 CE3 - COMUNICAÇÃO DIRETA LGPD – SOMOS OPERADORES

Após realizar as revisões de regulamentos e leis especialmente da própria LGPD, ficou claro para a empresa que a IPM Sistemas é considerada uma operadora nesse contexto. Com tal papel estabelecido, ficou evidente a necessidade da criação de um canal de comunicação direto de seus clientes e titulares de dados com a empresa.

Para isso fora criado um endereço de e-mail exclusivo denominado privacidade@ipm.com.br e realizada divulgação do mesmo nos documentos, sites, termos de uso e políticas de privacidade e uso aceitável do sistema.

4.11 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.

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 (Regulamento Geral sobre a Proteção de Dados – da União Européia) 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.

5 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, foi realizado um levantamento por meio de observação, 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 um total de 42 práticas relevantes à segurança da informação.

Com a identificação das práticas realizou-se a descrição sucinta de 11 delas que podem ser utilizadas e adaptadas para a realidade de outras empresas, por serem temas comuns para qualquer empresa de desenvolvimento de software.

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, com foco na manutenção da segurança e consequente privacidade das informações pessoais sob guarda da empresa.

6 REFERÊNCIAS

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

Fontes, E. (2006) Segurança da informação: o usuário faz a diferença. São Paulo. Saraiva.

GIL, Antonio Carlos. (2017) Como elaborar projetos de pesquisa. Rio de Janeiro. Atlas.

Goodrich, Michael T; TAMASSIA, Roberto. (2013) Introdução à segurança de computadores. Porto Alegre. Bookman.

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

ISO 15.408. (2009) Information technology — Security techniques — Evaluation criteria for IT security. https://www.iso.org/standard/50341.html, Outubro.

LGPD, Lei Geral de Proteção de Dados. (2018). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, Setembro.

Lyra, Mauricio Rocha. (2008) Segurança e Auditoria em Sistemas de Informação. Rio de Janeiro: Editora Ciência Moderna.

OWASP. (2021) Open Web Application Security Project. https://owasp.org/, Outubro.

Veloco, Thássius. (2010) O que é segurança da informação? https://tecnoblog.net/43829/o-que-e-seguranca-da-informacao/, Setembro.