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


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

FIRST 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/ clebernardelli@gmail.com

Resumo:
O primeiro de dois artigos com o principal objetivo de 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 em e-government. O Estudo de caso (pesquisa qualitativa) foi realizado em uma empresa que desenvolve Sistemas de Gestão de Governo Eletrônico ficando explicita a necessidade de adoção de práticas relacionadas a segurança da informação, proteção de dados pessoais e da privacidade de usuários, 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). O eixo Jurídico não foi subdividido. Essa abordagem permitiu uma maior cobertura de ações e identificação clara de cada prática adotada de forma individualizada, enumerando-as sequencialmente dentro de cada área. 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 primeiro artigo serão abordadas as primeiras 20 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 first of two articles with the main objective of describing 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, which makes clear the need to adopt practices related to information

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

security so that it would adhere 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. Based on this observation of security practices, a thematic model was developed having as axes: Technical, Cultural/Personal and Legal, then for each axis a subdivision into more specific areas was carried out, resulting in the following areas: Development , Product and ICT (in the Technical axis), Internal and External (in the Cultural/Personal axis). The Legal axis was not subdivided. This approach allowed for greater coverage of actions and a clear identification of each practice adopted individually, listing them sequentially within each area. In all, 42 practices were identified in use, some of which were adopted exclusively by the advent of security focused on the LGPD and others already existed, being modified as necessary. Finally, all practices were described individually. In this first article, the first 20 practices analyzed 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 lógicos 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 E SEGURANÇA DA INFORMAÇÃO

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
Compartilhar conhecimento é conhecer o mundo.
unisociesc

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).

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.

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

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

segurança da informação, manutenção da privacidade de dados e LGPD, a partir da revisão da literatura. Na 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 observação onde o pesquisador pode ser definido como um participante completo, por fazer parte do quadro de empregados da empresa.

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.

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.

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

	(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 Pessoais	(TT4) Mapeamento de ações: Antes, Durante e Depois de Incidentes	(CI4) Modificações no Manual do Colaborador	(CE4) Necessidade de Backup e Gestão Local do Cliente	(J4) Elaboração de Termo de Responsabilidad 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					

Quadro 1 - Distribuição Temática das Práticas
Fonte: Acervo dos Autores

Buscando melhorar ainda mais na identificação de cada prática observada, elas foram codificadas e sequenciadas cada uma em seu eixo/área. Nesse artigo a primeira parte delas foram descritas de forma sucinta até a linha 4 do Quadro 1. itens (TD4) Repositórios Internos Apenas (TP4) Mapeamento de Tratamentos de Dados Pessoais, (TT4) Mapeamento de ações: Antes, Durante e Depois de Incidentes, (CI4) Modificações no Manual do Colaborador, (CE4) Necessidade de Backup e Gestão Local do Cliente, exceto a coluna Jurídico, esse e demais itens serão descritos no segundo artigo por questões relacionadas ao tamanho máximo de páginas.

Algumas técnicas, ferramentas e suas versões, bem como o método exato de como elas são aplicadas, foram intencionalmente suprimidas.

5. RESULTADOS E DISCUSSÕES

5.1 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, cuja objetivo principal é descrever um conjunto de regras, boas práticas e ferramentas que devem ser adotados no ciclo de vida de desenvolvimento e manutenção de software.

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. Além da auditoria também existe o registro formal do uso da fonte externa realizado pelo próprio programador na ferramenta interna de trabalho.

Por questões de sobrecarga de gestão, pequenos trechos de código ou dicas de programação obtidas dessas fontes, não estão sujeitas a essa auditoria, porém como prática, aconselha-se fortemente que seja realizada revisão de código por outro programador ou analista da área afim.

Sobre esse aspecto ainda, 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 – PSI, 2020, p. 15).

5.2 TD2 - ADOÇÃO DO SECURITY BY DESIGN

Uma vez estudado e compreendidas as premissas do uso do Security By Design, uma série de medidas foram adotadas, entre elas (1) a elaboração de padrão de desenvolvimento exclusivo com foco em segurança da informação, (2) a execução de atividades de capacitação de colaboradores com foco em LGPD e segurança da informação, (3) a modificação do Framework de propriedade da própria empresa visando o tratamento de dados tanto no Front-End como no Back-End, com vistas a identificação e validação de tipos de dados, (4) engenharia reversa e verificação da arquitetura das aplicações, cuja objetivo foi identificar vulnerabilidades pré-existentes no projeto arquitetônico.

Deve-se considerar para essa prática que segurança não é uma *Feature* ou Funcionalidade específica do produto de software, mas sim um requisito não funcional ou uma qualidade esperada dele.

5.3 TD3 - CONTROLE DE CHAVES DE CRIPTOGRAFIA

Trata-se de uma prática amplamente difundida na segurança da informação, que chaves de criptografia não podem estar disponíveis de forma completa e/ou de produção dentro de códigos fonte. É necessário que o administrador seja capaz de definir chaves próprias no momento da instalação do sistema.

Desta forma foram realizados ajustes no sistema, para: (1) Criptografar todo conteúdo de chaves/senhas que é armazenado no banco de dados, (2) Chaves de criptografia que estavam embutidas nos códigos fonte foram “movidas” para arquivos de configuração e (3) Mecanismo de criptografia de senhas de usuários fora totalmente modificado, onde para cada cliente (mesmo que a senha seja igual a de outro usuário), exista um SALT específico e com isso um conjunto de caracteres totalmente diferente seja armazenado no banco de dados.

5.4 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.

5.5 TP1 - ADOÇÃO DO PRIVACY BY DEFAULT

Conforme descrito na fundamentação, 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.” (PSI IPM Sistemas, 2020, p. 21).

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

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.

Dentre os critérios de segurança que estão cobertos pelo nível forte destacam-se:

- Validar funcionário ativo no login – com base em informações do RH;
- Bloquear login por tentativa de acesso – Número de Tentativas 3 (padrão);
- Efetuar logoff automático com tempo de Inatividade (máx): 60 minutos;
- Regras de Composição de Senha: Mínimo de caracteres: 8, Nível de segurança: Forte:
    - Validação da quantidade mínima de caracteres (8);
    - Deverá incluir letras (necessariamente maiúsculas e minúsculas), números e caracteres especiais (como @!?%*);
    - A senha não poderá conter a data de nascimento da pessoa ou mesmo o código do usuário;
    - Ao alterar a senha, esta também não poderá ser igual a alguma das últimas cinco fornecidas.;
- Expirar senha de Novos Usuários;
- Intervalo padrão de Expiração: 90 dias (máximo).

Além disso, deve-se prever também por padrão comunicação por HTTPS, incluindo outras regras exclusivas de rede.

5.6 TP2 - PROATIVIDADE NO MONITORAMENTO DATA CENTER

O monitoramento do comportamento de redes de dados em Sistemas de Informação é fundamental, sendo o objetivo principal identificar qual é o comportamento normal da rede. Com base nesse funcionamento normal, fica mais evidente quando um possível ataque está sendo realizado, pois houve um aumento significativo do trafego de dados.

O mesmo princípio pode ser aplicado na medição de qualquer outro item do sistema, como espaço disponível em discos nos servidores, áreas de armazenamento temporário, áreas de log, etc.

Embora possa parecer algo com pouco relacionado a privacidade de dados, essa ação tem muito reflexo na segurança da informação, sendo este último necessário para que haja o primeiro. Um ataque de DDoS[1] pode ser identificado e tratado mais rapidamente se houver monitoramento.

[1] Uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede.

Um conjunto de ferramentas de monitoramento é recomendado. No caso concreto, observa-se o uso da ferramenta Zabbix, que permite elaborar mapas, visualizações e alertas sofisticados por meio de dados obtidos pelos agentes que ficam residentes nos mais diversos servidores.

5.7 TP3 - POLÍTICA DE ACESSO USUÁRIO NORMAL X TÉCNICO

Essa iniciativa tem como princípio a não criação de usuários nos sistemas/bases de dados de produção, para fins de manutenção do sistema. O usuário técnico de manutenção (empregado da empresa), faz sua autenticação nos sistemas por meio de um mesmo login único exclusivo dele. Esse login é o mesmo utilizado nas ferramentas internas e uma checagem de privilégios e a sua condição funcional (se está empregado, em jornada de trabalho, em férias, afastado, etc.) é realizada em um serviço (API) da própria empresa.

Em síntese, para poder realizar acesso em sistemas de (seja de produção ou não), um empregado deverá estar trabalhando, dentro de sua jornada de trabalho e deverá ter os privilégios necessários para tal.

Ao ser realizado desligamento do empregado, o próprio setor de RH ao realizar os procedimentos já dispara ação automática que desativa o usuário dele, sendo que imediatamente ele não consegue mais acessar nenhuma das bases que possuía acesso.

5.8 TP4 - MAPEAMENTO DE TRATAMENTOS DE DADOS PESSOAIS

Seguindo instruções disponibilizadas pelo Governo Federal, por meio do Guia de Elaboração de Inventário de Dados Pessoais[2], 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

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

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

do guia, sendo identificadas 64 categorias diferentes. Uma categoria de dados em especial, trata daqueles denominados sensíveis.

5.9 TT1 - ELABORAÇÃO E PUBLICAÇÃO DO PSI E DOCUMENTOS DERIVADOS

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, conforme pode ser visto na Figura 3.

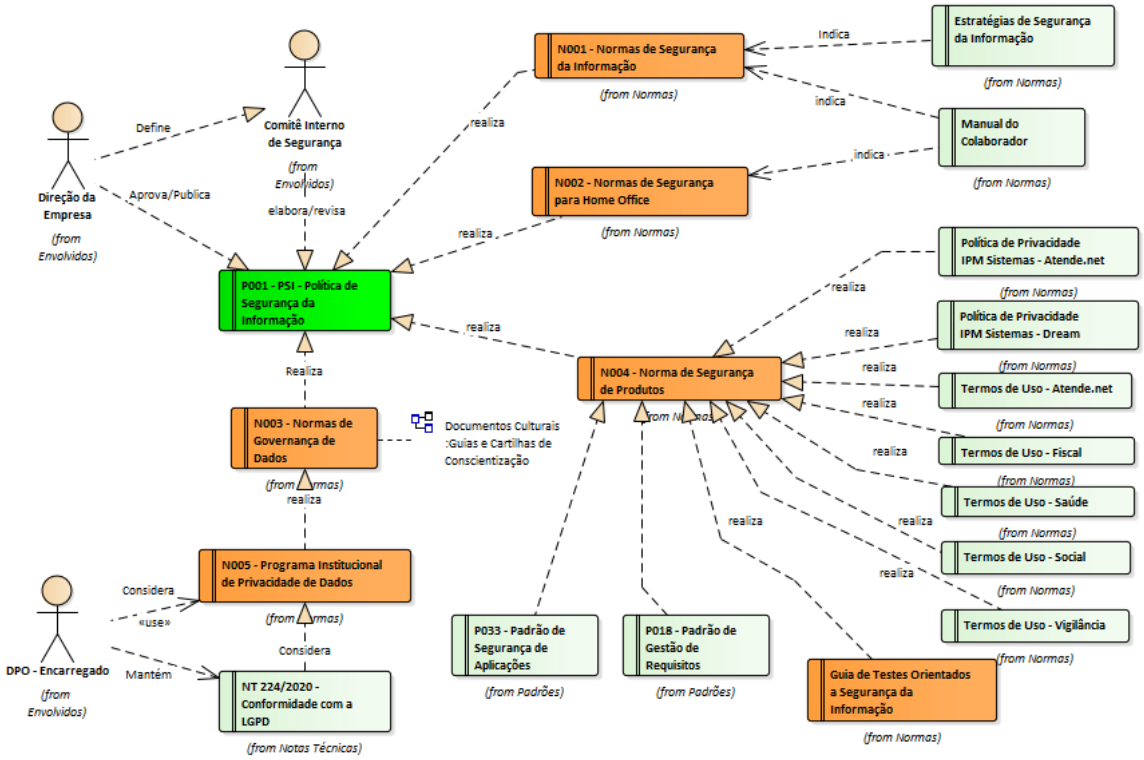


Figura 1 - Documentos Derivados da PSI

Fonte: PSI da empresa.

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

5.10 TT2 - SEGMENTAÇÃO DE REDES

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

Um aspecto fundamental de qualquer ambiente de desenvolvimento de software seguro é a separação de redes. No caso da empresa as redes de Desenvolvimento, Teste/Qualidade e ambiente de Produção são totalmente distintos. Um dos principais motivadores dessa prática é que não haja acesso de pessoas fora do time aos artefatos do projeto, que possam fazer alguma mudança inesperada no ambiente, como a injeção de um código malicioso intencional, ocultando-o dos demais membros.

Vale lembrar que as redes não possuem qualquer relação, ou seja, estão separadas fisicamente.

5.11 TT3 - ACESSO FÍSICO E LÓGICO CONTROLADOS

Conforme a ISO/IEC 15.408, essa também é uma prática aconselhada, quando se restringe o a cesso físico e lógico aos ambientes. O uso de um sistema de controle de domínio, como o Windows Active Directory se faz necessário nesse sentido.

Na empresa verifica-se que em mesmo estando segmentadas as redes, existe um controlador de domínio para cada uma, e as políticas de segurança são aplicadas por meio de GPOs[3].

As políticas são definidas com base no documento N001 (Normas de Segurança da Informação), definido no PSI. Entre as regras está a obrigatoriedade de mudança de senha a cada 60 dias, uso de senhas fortes, restrição de uso de senhas anteriores e restrição para compartilhamento e mapeamento de unidades de rede.

5.12 TT4 - MAPEAMENTO DE AÇÕES: ANTES, DURANTE E DEPOIS DE INCIDENTES

Trata-se da elaboração de um documento que descreve como devem ser conduzidas as ações de avaliação de risco, incluindo atividades a serem conduzidas antes (para detecção de possíveis vulnerabilidades e incidentes), durante (mecanismos de medição e ativos de informação mais relevantes a serem protegidos) e depois (mapeamento de ações realizadas e medidas preventivas a serem adaptadas ou incluídas). No PSI da empresa, esta diretriz está descrita da seguinte forma “devem ser conduzidas avaliações de risco, periodicamente, a fim de mensurar eventuais vulnerabilidades, sendo esta atividade definida pelo documento N001 - Normas de Segurança da Informação em seção exclusiva”. (IPM Sistemas - PSI, 2020, p. 2).

[3] Um conjunto de configurações que permite ao administrador personalizar diversos recursos dos usuários e dos computadores seja localmente (stand-alone) ou em um ambiente do domínio.

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

Desta forma com a criação da norma N001, observa-se na empresa ações e medidas que estão sendo conduzidas especialmente pela área de Tecnologia da Informação, pois neste caso as medidas dizem respeito aos ativos de informação da empresa e não relação direta ao produto. Para este caso especificamente, de acordo com o PSI elaborou-se a N004, já mencionada anteriormente.

5.13 CI1 - AÇÕES DE CAPACITAÇÃO DE PESSOAL

Conforme descrito por DRUMMOND (2020) e referenciado na revisão da literatura, “No contexto laboral e corporativo, a LGPD se aplica à toda a equipe”. Em se tratando de Segurança da Informação é sabido que o elo mais fraco normalmente está relacionado ao despreparo das pessoas envolvidas. Soma-se a isso, o déficit cultural relacionado diretamente a segurança em meios digitais que existe em praticamente todo lugar do mundo. Em virtude disso é imprescindível um trabalho de capacitação de pessoal adequado.

Observa-se na empresa que já foram realizadas ações de treinamento presencial com seus colaboradores acerca da LGPD e temas ligados a segurança da informação. Além disso, observa-se também atenção especial a contratação de pessoal onde são informados aos novos colaboradores quais são os princípios fundamentais ligados ao tema.

5.14 CI2 - CAMPANHAS DE CONSCIENTIZAÇÃO INTERNAS

Como forma de aplicação das políticas do PSI, uma série de campanhas internas de conscientização são realizadas. Até o momento já foram publicadas 4 cartilhas orientativas, sendo enviadas via e-mail para os colaboradores, conforme exemplo na Figura 4.

Além disso, publicações em mídias sociais externas e internas foram realizadas, com vistas a segurança da informação.

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

Figura 2 - Exemplos de Cartilhas de Segurança

Fonte: Catalogo de Cartilhas da Empresa.

Essas cartilhas fazem parte de um conjunto maior de ações de aculturamento interno de segurança da informação, como as ações de Capacitação. A distribuição desse material ocorre de forma cíclica, com vistas a novos empregados.

5.15 CI3 - COMUNICAÇÃO DIRETA LGPD – SOMOS OPERADORES

A cultura externa da empresa quanto a LGPD, passa pelo entendimento primeiro de que ao ser operadora ela possui responsabilidade e sendo assim as ações se justificam. Em outras palavras, ao se identificar desta forma todos os envolvidos devem estar atentos as políticas e normas da empresa.

Mas o foco principal dessa prática observada é outro: O cliente. É necessário que a empresa não só produza software com funcionalidades que contenham recursos seguros, mas também haja proativamente comunicando seus clientes de que a LGDP existe, do que se trata, que já entrou em vigor e que está pronta para auxiliá-los.

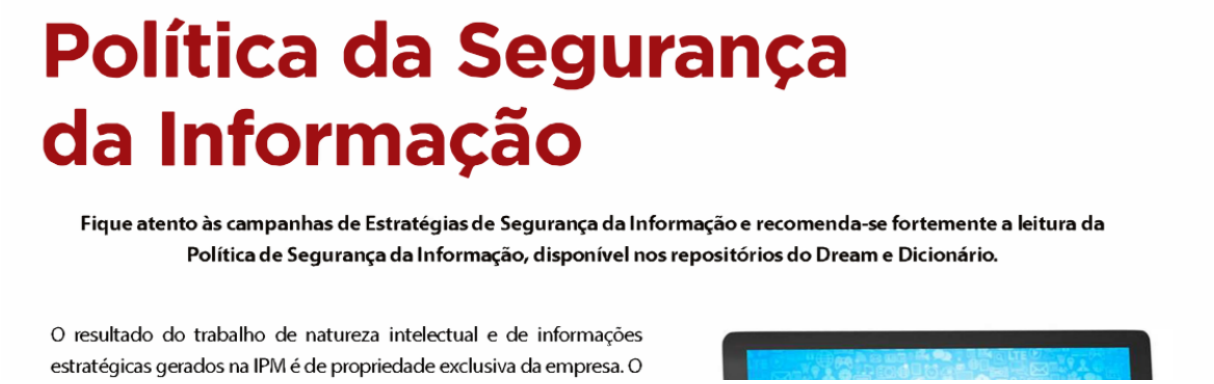
Sendo assim, um oficio foi enviado para todos os clientes, com essa abordagem, indicando ações de segurança já adotadas (Privacy By Default) e se colocando a disposição para auxiliar na implantação das práticas exigidas pela lei, como transparência Ativa e Passiva, por meio da plataforma de Autoatendimento e Cadastro Único.

5.16 CI4 - MODIFICAÇÕES NO MANUAL DO COLABORADOR

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

Como consequência da criação do PSI, o documento manual do colaborador teve que ser ajustado fazendo referência ao documento e, de forma geral, as diretrizes fundamentais. É necessário que o colaborador saiba da existência da tais regras e o manual do colaborador é um elemento fundamental para a disseminação dessa informação.

É necessário no entanto, que os colaboradores tenham acesso ao documento assim que forem admitidos na empresa e também a qualquer momento, quando acharem necessário. No cenário da empresa o documento é entregue ao colaborador na admissão e também fica disponível para download a qualquer tempo no repositório de documentos. Pode-se observar um fragmento do documento na Figura 5.


Política da Segurança da Informação

Fique atento às campanhas de Estratégias de Segurança da Informação e recomenda-se fortemente a leitura da Política de Segurança da Informação, disponível nos repositórios do Dream e Dicionário.

O resultado do trabalho de natureza intelectual e de informações estratégicas gerados na IPM é de propriedade exclusiva da empresa. O

Figura 3 - Parte do Manual do Colaborador – Segurança

Fonte: Manual do Colaborador da Empresa.

Esse repositório de documentos, pode ser desde uma aplicação web acessível aos colaboradores, como uma pasta na rede contendo os documentos.

5.17 CI5 - ANONIMIZAÇÃO DE DADOS PESSOAIS EM DEMONSTRAÇÕES

Essa prática foi classificada no grupo da Cultura Interna, pois é dever dos colaboradores observar a ações de anonimização de dados a serem aplicadas em ambientes de demonstração de produto. Esses ambientes normalmente utilizam-se de bases de dados de clientes, que foram restauradas afim de dar mais credibilidade as operações realizadas no sistema, como o volume de dados utilizado. No entanto observou-se nesse contexto que inúmeros dados pessoais eram expostos durante as sessões de demonstração.

Com base nessa constatação fora desenvolvido uma ferramenta de software para ser utilizada exclusivamente no processo pós-restauração dessas bases de dados, com objetivo de reconfigurar e anonimizar.

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

5.18 CE1 - FOCO NA PREVENÇÃO DE INCIDENTES

As ações do grupo cultural externas foram focadas nos usuários e administradores locais do sistema, deste modo elas atuam sob o ponto de vista de prevenção e conscientização. O fato de fornecer software no modelo SaaS (Software como Serviço, do inglês *Software As An Service*), denota sobre a empresa a necessidade de um trabalho adicional com vistas a proteção e segurança do sistema, o que resulta também em ações que fortalecem a privacidade do usuário.

Não basta que a infraestrutura e o software possuam mecanismos de segurança, se não há prevenção nesse mesmo enfoque pelos seus usuários. Isso fica evidente quando muitos dos clientes oficiam a empresa solicitando para que os níveis de segurança possam ser administrados por eles, afim de que certas concessões possam ser realizadas.

Quando isto ocorre cabe a empresa indicar os motivos de tais recursos de segurança adicionais e potenciais riscos em não os observar.

5.19 CE2 - POR QUE SE PREOCUPAR COM SEGURANÇA?

São vários os fatores que podem justificar tal preocupação:

- Punições e/ou sansões legais;
- Suspensão de serviços por mandado judicial;
- Exposição de dados pessoais e sensíveis de terceiros;
- Indisponibilidade temporária ou permanente de serviços por questões técnicas, como sequestro de dados (*Ransonware*);
- Fraudes geradas por terceiros por meio do mal uso ou armazenamento em local inseguro de credenciais de acesso (login e senha de usuário);
- Roubo de identidade (agravada pelo fato anterior);
- Extorsão (sequestro de dados ou dados confidenciais obtidos de forma ilegal);
- Sextorsão (tipo de extorsão causada pela obtenção ilegal de imagens ou vídeos íntimos de pessoas);
- Roubo de dados sigilosos e/ou confidenciais;

Esses são apenas alguns dos diversos motivos. Mas o objetivo da empresa nesse sentido não é causar pânico nas pessoas, usuários e administradores, mas sim conscientiza-los da necessidade de pensar em segurança proativa.

Por parte da empresa é nítida a percepção de que essas camadas de segurança impactam também na imagem da empresa perante seus clientes, empregados e a sociedade como um todo.

5.20 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.

5.22 CE4 - NECESSIDADE DE BACKUP E GESTÃO LOCAL DO CLIENTE

Embora haja toda uma infraestrutura e ações permanentes para realização, teste e armazenamento de backups dos dados, a empresa disponibiliza um portal onde o cliente pode verificar e realizar download dos backups para armazenamento local ou até mesmo em outro provedor de armazenamento em nuvem.

Para demonstrar ao cliente a importância do tema, um oficio é enviado para os clientes indicando a necessidade de nomear um responsável, dando-lhe as credenciais para que faça acesso ao portal e realize o acompanhamento.

Por outro lado, para evitar problemas como vazamento de dados, os backups são compactados com senha individual por cliente e o acesso a plataforma de download somente pode ser feito de forma autenticada por meio de assinatura digital utilizando-se de um certificado do tipo A3 (ICP-Brasil) que é acessível apenas em meio físico.

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 primeiras 20 práticas evidenciadas nesse primeiro artigo 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. As demais práticas serão descrita no segundo artigo.

REFERÊNCIAS

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.

CYBER SECURITY AGENCY OF SINGAPORE (CSA). **Security-by-Design Framework** Versão 1.0. Singapura, 2017. Disponível em: <https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.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.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** Rio de Janeiro: Atlas, 2017.

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

HOPPEN, Norberto; LAPOINTE, Liette; MOREAU, Eliane. **Um guia para avaliação de artigos de pesquisas em sistemas de informação**. READ: revista eletrônica de administração. Porto Alegre. Edição 3, vol. 2, n. 2 (set/out 1996), documento eletrônico, 1996.

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.