CURSO DE TECNOLOGIA EM DEFESA CIBERNÉTICA

CAP 8 - LGPD: E AGORA? - ADEQUANDO O CLIENTE PARA A LGPD

SÃO PAULO – SP

ABRIL/2021

AGATHA NOGUEIRA

CLEIBSON MARTINS

GILBERTO RIBEIRO BARBOSA

GUILHERME PEREIRA DA SILVA NETO

IAN ALBERTO RIBEIRO CHRISTANI

CAP 8 - LGPD: E AGORA? - ADEQUANDO O CLIENTE PARA A LGPD

SÃO PAULO – SP

ABRIL/2021

SUMÁRIO

1. INTRODUÇÃO

A atual transformação digital tornou os dados um ativo altamente valioso. A frase “dados são o novo petróleo" é a mais nova realidade, principalmente quando falamos em segurança da informação e defesa cibernética.

Cibercriminosos usam as informações garimpadas na internet como ferramentas de ataques, seja em engenharia social, malwares ou até mesmo em brute force. Portanto deve-se adotar uma gestão e controle sobre os dados coletados e disponibilizados por instituições, aplicativos e etc.

Pensando nessa gestão, a Lei Geral de Proteção a Dados (LGPD) foi criada em 2018 e sancionada em agosto/2020 no Brasil, porém multas e sanções só poderão ser aplicadas a partir de agosto/2021. A lei nada mais é que uma regulamentação para o uso de dados de pessoas físicas, com o objetivo principal de proteger a privacidade dos consumidores e cidadãos. E essa proteção vem através de mudanças na forma de coletar, armazenar e usar os dados das pessoas.

Com a LGPD muitas empresas precisarão se adequar para implementar os novos processos necessários e é esse o tema da atividade: **CAP 8 - LGPD: E AGORA? - ADEQUANDO O CLIENTE PARA A LGPD.** Ao longo deste trabalho vamos pontuar os principais campos para montar o relatório RIPD e iniciar o cliente no mundo da LGPD.

2. DADOS POR DEPARTAMENTO

Neste capítulo vamos descrever a corrida do laboratório Hígia Bolzachini para se adequar à LGPD e o passo inicial é a confecção do RIPD com os seguintes campos por departamento: titular e dados coletados, finalidade e forma da coleta, tempo de armazenamento, controles de segurança e compartilhamento.

Para visualizar essas informações organizadas em forma de planilha, conferir a seção Anexo.

2.1. RH

A função do departamento de Recursos Humanos é gerenciar os interesses dos funcionários e os da empresa. Sendo responsáveis por todo o processo de admissão e demissão, folha de pagamento, benefícios e atratividade.

Os principais **dados coletados** são: dados pessoais (nome, endereço, data de nascimento, CPF, RG, CTPS, formas de contato), dados financeiros (remuneração, conta bancária, empresas e sócios), dado referentes à família, histórico profissional e acadêmico, histórico de saúde e dados de diversidade (raça, religião, orientação sexual, deficiências).

Estes dados foram **coletados** através da aplicação de questionários, de entrevistas a fim de averiguar e compreender opiniões, ações e condutas, da observação de comportamento a fim de trabalhar meios científicos (feedbacks) e também através de e-mails e SMS.

Eles foram coletados com as seguintes **finalidades:** transferência de arquivos físicos para sistemas especializados em tratamento de dados, promover as informações para cumprimento de contrato, cumprimento da obrigação legal, dados coletados e informações para defesa de processos judiciais.

Após a coleta **devem ser retidos** por no mínimo 5 anos em sistema interno próprio e criptografado.

Como **controles de segurança** devem ser implantados programas de governança de privacidade e checagem de background para os novos colaboradores.

Se necessário, o **compartilhamento** será feito com instituições como INSS, Governo, hospitais (em caso de emergência no serviço) e polícia (caso de investigações).

2.2. TI

Com a evolução das tecnologias na sociedade e também com a LGPD, o departamento de TI se transformou em uma das áreas mais estratégicas da empresa, sendo o responsável por todos os sistemas e infraestrutura tecnológica do laboratório, como servidores, websites, APPs, acessos à internet e aos sistemas internos.

Os principais **dados coletados** pelo departamento são credenciais, listas de acessos, contas de e-mail, biometria, senhas para dispositivos de rede, nome e sobrenome, cargos, servidores, hosts e IPs.

Estes dados foram **coletados** através da coleta presencial com o colaborador e programas de mapeamento.

E as principais **finalidades** para coleta foram: a criação de contas de email, configuração de computadores, configuração das políticas de TI da empresa e controle de acesso (tanto físico quanto digital).

Os dados deverão ser **retidos** por no máximo 3 anos após o desligamento do colaborador e armazenados em servidores de backup e também em serviços de armazenamento em nuvem (ex. AWS).

Como **controles de segurança** devem ser implantados políticas de segurança, mitigação de pontos de falhas, fazer monitoramento da rede, usar a política de acesso mínimo aos colaboradores, determinar horários em que os servidores podem ser acessados, usar lista de controle de acessos, criptografar formas de comunicação (inclusive e-mails), acesso restrito ao local de servidores, backups feitos regularmente, ter planos de recuperação e defesa contra ataques.

Se necessário, o **compartilhamento** será feito com a polícia em caso de investigações.

2.3. FINANCEIRO

O departamento financeiro é responsável pela gestão das finanças do laboratório, exercendo a contabilidade, tesouraria e gestão de custos. Efetuando, por exemplo, convênios, fluxo de caixa, pagamentos e recebimentos.

Os principais **dados coletados** pelo departamento são os nomes de funcionários, clientes, fornecedores, dados financeiros, fluxo de caixa e condição financeira atual da empresa.

Estes dados foram **coletados** através da coleta presencial diretamente com os colaboradores, clientes e fornecedores, também mediante a apresentação de comprovantes, e mails, notas fiscais, aplicativos e bureaus externos.

E as principais **finalidades** para coleta foram: cumprimento de obrigação legal ou regulatória, estudo realizado por órgão de pesquisa, proteção do crédito, balanço financeiro e prospecção de clientes e mercado.

O tempo de retenção dos dados financeiros é bem diversificada, sendo 5 anos para adiantamento salarial, 10 anos para pagamento de férias e salários, 10 anos para comprovantes de pagamento de INSS, 5 anos para COFINS e DARF, 30 anos para depósitos de FGTS e 5 anos para declaração de IR.

Como **controles de segurança** devem ser aplicadas listas de controle de acesso aos dados limitando a gerentes setoriais, seus eventuais substitutos e aplicação de anonimização na identificação de terceiros, assim como também restrição de acesso físico para o ambiente financeiro.

Se necessário, o **compartilhamento** será feito com o Governo, Laboratório Double Helix, Convênios Médicos, Contabilidade, Fornecedores, Jurídico e polícia.

2.4. ATENDIMENTO AO CLIENTE

No laboratório, como na grande maioria das empresas, o departamento de Atendimento ao Cliente tem destaque pois é responsável pela gestão do relacionamento com o cliente como um todo, desde o atendimento, orientação, captação e até a fidelização dos clientes.

Os principais **dados coletados** pelo departamento são os dados pessoais dos clientes (nome, data de nascimento, endereço, CPF), dados de identificação (e-mail, telefone, redes sociais) e dados de pagamento (cartão, convênios).

Estes dados foram **coletados** através no momento do atendimento de forma presencial mediante identificação pessoal comprovada e por aplicativos de cadastro online.

E as principais **finalidades** para coleta são: execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular a pedido do titular dos dados, tutela da saúde, identificação em consultas futuras, histórico médico e fidelização do cliente.

O tempo de **retenção** dos dados coletados no atendimento é de 20 anos.

Como **controles de segurança** devem ser aplicados métodos anonimização por hash no documento do cliente e controle de acesso aos dados.

Se necessário, o **compartilhamento** será feito com o Órgão regulador, Laboratório Double Helix e Convênios Médicos.

2.5. MEDICINA DIAGNÓSTICA

O departamento de Medicina Diagnóstica é o responsável por proporcionar a assistência ao paciente na classificação de sua condição de saúde, através de serviços, exames, tratamentos e diagnósticos.

Os principais **dados coletados** pelo departamento são os históricos relativo à saúde do paciente, guias de exame com informações pessoais (nome, data nascimento, endereço), dados de pagamento (numero convenio, cpf, forma de pagamento) e informações do procedimento (quando, como e onde), resultado dos exames em forma digital e quadro clínico.

Estes dados foram **coletados** no momento do atendimento de forma presencial mediante identificação pessoal comprovada, através de formulários impressos, resultados de exames, por aplicativos de cadastro online e em websites/e-mails.

A principal **finalidade** para coleta é o uso de dados em técnicas dedicadas ao paciente e aos exames que complementam, monitoram e dão auxílio ao diagnóstico, tratamento e prognóstico.

O tempo de **retenção** dos dados coletados no diagnóstico médico é de 20 anos.

Como **controles de segurança** devem ser aplicados métodos anonimização por hash no documento do cliente, controle de acesso aos dados em arquivos físicos, separação dos dados em rede diferente das demais e o acesso feito via autenticação com duplo fator.

Se necessário, o **compartilhamento** será feito com laboratórios parceiros, como Double Helix, e Convênios Médicos.

2.6. COMPRAS

O departamento é o responsável pela gestão de compras e negociações com os fornecedores, para suprir a necessidade de suprimentos do laboratório. Como, por exemplo, adquirir materiais (escritório, médico, comunicação), mercadorias e equipamentos médicos e de TI.

Os principais **dados coletados** pelo departamento são os dados financeiros de fornecedores e de caixa do laboratório.

Estes dados foram **coletados** por aplicativos e planilhas de controles, notas fiscais, orçamentos, agenda de contatos/representantes, validades e emails.

A principal **finalidade** para coleta é o uso de dados em aquisições de materiais para o laboratório, como novos equipamentos médicos e materiais de consumo diário, desde materiais hospitalares até objetos comuns como papel e caneta. Junto ao departamento de Manutenção faz-se a aquisição de peças sobressalentes para eventuais reparos de equipamentos de manutenção. Fatores fundamentais para o setor de compras: Recebimento e armazenamento dos produtos, constatação de preço, prazo e qualidade, aprovação de pagamento para o fornecedor e realizar análise dos dados de compras.

O tempo de **retenção** dos dados coletados no departamento é de 5 anos.

Como **controles de segurança** devem ser a aplicação de lista de controle de acesso aos dados limitando a gerentes setoriais, seus eventuais substitutos e aplicação de anonimização na identificação de terceiros.

Se necessário, o **compartilhamento** será feito com o Governo, Laboratório Double Helix, Convênios Médicos, Contabilidade, Fornecedores.

2.7. MANUTENÇÃO

O departamento é o responsável por organizar planos de manutenção e reparo de equipamentos e instalações e, também, gerir a execução e eficiência de técnicos. Em parceria com o departamento de Compras, faz a aquisição de peças para consertos de equipamentos defeituosos.

Os principais **dados coletados** pelo departamento são dados de inventário que contém descrição de dispositivos e sistemas usados

Estes dados foram **coletados** por arquivos, aplicativos e planilhas de controles, listas de espera e base de dados.

A principal **finalidade** para coleta é a manutenção e continuidade dos negócios.

O tempo de **retenção** dos dados coletados no departamento é o tempo de duração do equipamento e os dados compartilhados com compras e TI devem seguir o prazo estipulado pelo departamento.

Como **controles de segurança** devem ser a aplicação de lista de controle de acesso aos dados limitando a gerentes de TI e Compras, seus eventuais substitutos e aplicação de anonimização na identificação de terceiros.

Se necessário, o **compartilhamento** será feito com a polícia, em caso de investigação.

2.8. COMERCIAL

Assim como o departamento de atendimento ao cliente, é o responsável pelo relacionamento com os clientes. Gerindo custos e investimentos, carteiras, rotinas de vendas, marketing, parcerias, prospecção de mercados e clientes.

Os principais **dados coletados** pelo departamento são contatos de terceiros, nomes de representantes e empresas em que trabalham, dados e preferências dos clientes para fidelização e benefícios, carteiras de contatos e clientes.

Estes dados foram **coletados** por aplicativos e planilhas de controles, notas fiscais, orçamentos, agenda de contatos/representantes

A principal **finalidade** para coleta é a manutenção e continuidade dos negócios, análise de dados e perfil, CRM e auditoria.

O tempo de **retenção** dos dados coletados no departamento é de 5 anos.

Como **controles de segurança** devem ser a aplicação de lista de controle de acesso aos dados limitando a gerentes setoriais e seus eventuais substitutos.

Se necessário, o **compartilhamento** será feito com a polícia, em caso de investigação.

3. CONCLUSÃO

Os vazamentos de informações de grandes e relevantes instituições nos mostram que quanto mais avançamos e estreitamos as relações digitais, mais fornecemos dados às instituições e, consequentemente, mais expostos estamos.

Para prevenir e evitar cenários catastróficos de vazamentos de dados, a LGPD vem para normatizar a coleta, consumo e armazenamento dos dados de pessoas físicas por parte de pessoas jurídicas.

Assim como neste trabalho, em que fizemos a introdução do laboratório Hígia Bolzachini no processo de LGPD, é essencial para nós, estudantes de defesa cibernética, ter o conhecimento em direito digital e em LGPD, para exercer atividades de implantação, melhorias, adequação e gestão em empresas.

REFERÊNCIAS

ABLAS, Barbara. **O que é LGPD? Cinco perguntas e respostas para se adequar à nova lei.**

https://www.techtudo.com.br/noticias/2020/08/o-que-e-lgpd-cinco-perguntas-e-respostas-para-se-adequar-a-nova-lei.ghtml

BARBOSA, Daniel. **8 ferramentas de adequação à Lei Geral de Proteção de Dados (LGPD)**

https://www.welivesecurity.com/br/2020/09/22/8-ferramentas-de-adequacao-a-lei-geral-de-protecao-de-dados-lgpd/

Dados: o novo petróleo do mundo e combustível para o futuro. https://bakertillybr.com.br/dados-novo-petroleo/#:~:text=Em%20tradu%C3%A7%C3%A3o%20livre%20para%20o,sido%20bastante%20citada%20no%20mercado.

Entenda os impactos da Lei Geral de Proteção de Dados (LGPD). https://www.welivesecurity.com/br/2021/01/28/entenda-os-impactos-da-lei-geral-de-protecao-de-dados-lgpd/

FIAP. **Cap 1 - É a hora da LGPD!.** São Paulo: FIAP/Defesa Cibernética, 2021

FIAP. **CAP 8 - LGPD: E AGORA? - ADEQUANDO O CLIENTE PARA A LGPD.** São Paulo: FIAP/Defesa Cibernética, 2021

ANEXO

Segue dados descritos na atividade sumarizados e organizados em formato de planilha.

Arquivo Planilha_anexo_atividade_cap8