**Levantamento de Riscos por Área**

**[Modelo alternativo de documento para nortear a construção do seu RELATÓRIO DE IMPACTO]**

|  |
| --- |
| **Definição** |
| Esse documento foi criado com o intuito de levantar informações para a implementação da **Lei Geral de Proteção de Dados**, a [**LGPD**](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm).  Em linhas gerais, a **LGPD** determina sobre o consentimento da coleta e tratamento de dados de pessoas físicas, isso engloba, quais informações as empresas podem coletar, de que maneira isso poderá ser feito e que tipo de autorização o consumidor tem que manifestar. Além disso, quanto tempo esses dados poderão ficar armazenados e para qual utilidade, e ainda, a possibilidade de revogação do consentimento de posse. |

|  |
| --- |
| **Objetivo** |
| Esse documento serve como apoio para você levantar os principais riscos que sua empresa pode estar exposta com a LGPD. Para isso, é feito um detalhamento sobre todos os dados INCLUSIVE sensíveis identificados em cada área e atividade da sua empresa. **Esse levantamento tem o objetivo final de criação de um Plano de Ação rápido para a adequação à lei.** |

|  |
| --- |
| **Instruções** |
| É recomendável que esse levantamento seja feito em todas as áreas da sua empresa, por um representante de cada setor. Para cada área será elaborado um documento. Assim, ao final você conseguirá identificar melhor quais delas possuem maiores riscos e por onde você deve começar seu plano de ação de adequação à lei.  Sugerimos que você reúna os responsáveis de cada área para fazer uma reunião explicando o objetivo do documento e o passo a passo para preenchimento.  Em cada tópico você terá uma breve explicação de como preenchê-lo.  São eles:   1. Grupos de Dados: agrupamento por tipos de dados sensíveis usados na empresa. 2. Atividades do setor: levantamento de todas as atividades do setor e quais dados essa área tem acesso, porque e como os utiliza. 3. Mapa de Dados: mapeamento de todos os dados usados em cada atividade, com informações de armazenamento e finalidade de uso. 4. Assessment de Riscos: encontrar possíveis gaps de uso dos dados sensíveis, por exemplo, finalidade de uso dos dados, necessidade, compartilhamento, transparência, qualidade dos dados e medidas de segurança. 5. Riscos Identificados: elencar os riscos identificados. |

**Histórico do Documento**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| É necessário manter um histórico, com os registros de criações e ajustes no documento. Isso servirá para acompanhar o andamento das atividades e possíveis alterações no escopo. Exemplo: | | | | |
| **Versão** | **Atividade** | **Descrição** | **Data** | **Responsável** |
| 1.0 | Redação | Elaboração Política / Norma |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |
| --- |
| 1. **Objetivos do Documento** |
| Este documento tem como objetivo avaliar e registrar onde são usados dados pessoais e sensíveis na empresa XPTO SEGURANÇA ELETRÔNCIA. Esse levantamento faz parte das práticas para adequação a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). |

|  |  |
| --- | --- |
| 1. **Grupos de dados** | |
| Para facilitar o levantamento de riscos, aconselhamos que você crie grupos de dados mais comumente usados. Indicamos que os grupos sejam separados por tipo de dados, isso irá te ajudar a relacionar e entender melhor os dados sensíveis que cada área trata. Veja alguns exemplos em azul: | |
| **Grupo** | **Dados Envolvidos** |
| Documentação | CPF, RG, Nro. Convênio Médico, Nro. Convênio Odontológico. |
| Dados pessoais | Nome, Data de nascimento, Sexo, Estado civil, Naturalidade, Nacionalidade, Etnia. |
| Dados familiares | Nome do cônjuge, Nome do pai, Nome da mãe, Nome dos filhos, Pensionista. |
| Contato | Telefone particular, Telefone corporativo, E-mail particular, Email corporativo. |
| Endereço | Endereço, Número, CEP, Bairro, Cidade, País, Complemento. |
| (Outros podem ser criados) |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Atividades do setor** | | | | |
| Nessa etapa, você deve elencar todas as atividades do setor em que está sendo avaliado. Esse trabalho é feito para entender quais dados são necessários para cada atividade, como estão sendo usados, quem tem acesso a eles e de quem são. É importante segmentar as atividades para que não se esqueça de nenhum dado. | | | | |
| **Atividade** | | **Cargo executante** | **Utiliza dados pessoais ou sensíveis?** | **De quem?** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |

|  |
| --- |
| 1. **Mapa de dados** |

|  |  |  |  |
| --- | --- | --- | --- |
| Baseado no levantamento do Tópico 2 (Atividades do Setor), você deve elencar todos os dados sensíveis e qual a finalidade dos dados identificados em cada atividade, isso irá facilitar o levantamento de riscos. Além disso, é necessário mapear onde estão armazenados esses dados, por quanto tempo e indicar se existe alguma lei ou consentimento que permita a sua captura. Essas são informações requeridas pela LGPD. | | | |
| **Finalidade**: Descreva aqui a atividade principal e seu objetivo. Pode ser mais de uma finalidade por atividade. | | | |
| **Dado** | **Base legal** | **Onde está armazenado** | **Período de armazenamento** |
| Nome |  |  |  |
| E-mail |  |  |  |
| Endereço |  |  |  |
| Telefone |  |  |  |
| Enfermidade |  |  |  |
| Uso de medicamento |  |  |  |

1. **Assessment Riscos**

|  |
| --- |
| Aqui entramos na parte primordial do documento: o levantamento de riscos. Deve-se apontar para quais finalidades os dados coletados serão usados. Caso não sejam usados ou usados diretamente na atividade indicada, deve-se explicar porque você deve ter posse daquele dado. |
| * 1. **Finalidade/Adequação** |
| *Os dados são utilizados para finalidades legítimas?* |
|  |
| *A finalidade é explícita e informada para o portador do dado?* |
|  |
| *Se a base legal é “Consentimento”, o titular tem como consentir, revogar seu consentimento e verificar quais os consentimentos dados, de maneira inequívoca?* |
|  |

|  |
| --- |
| Aqui você identifica se os dados são usados apenas quando necessário e por pessoas necessárias. |
| * 1. **Necessidade** |
| *Os dados são utilizados somente quando necessários?* |
|  |
| *Todos que utilizam os dados têm real necessidade?* |
|  |
| *Os dados são mantidos somente pelo tempo necessário?* |
|  |

|  |
| --- |
| Aqui você identifica se por algum motivo os dados são compartilhados com terceiros. Caso sejam, porque e com qual nível de segurança. |
| * 1. **Compartilhamento de dados?** |
| *Os dados são compartilhados com terceiros?* |
|  |
| *Se sim, existem medidas para garantir a segurança desses dados?* |
|  |
| *Se sim, existem meios para informá-lo sobre a solicitação de esquecimento do dado?* |
|  |

|  |  |  |
| --- | --- | --- |
| Elenque aqui quais terceiros têm acesso aos dados e quais dados são. | | |
| * + 1. **Terceiros** | | |
| **Parceiro** | **Tipo de parceria** | **Dados compartilhados** |
|  |  |  |

|  |
| --- |
| Uma das premissas principais da LGPD diz respeito ao consentimento e ao livre acesso a esses dados. Os donos têm direito de saber quais dados as empresas possuem, e também de retirar esse consentimento, de solicitar alterações, etc. Por isso, nessa etapa, você deve indicar mais informações sobre os dados que tem em sua base. |
| * 1. **Livre acesso** |
| *Está documentado a forma em qual formato estão dos dados? (formulário impresso, entrada de dados online, banco de dados, etc.)* |
|  |
| *Está documentado a forma como os dados são transferidos? (e-mail, correio, telefone, etc.)* |
|  |
| *Os processos onde os dados são utilizados estão documentados?* |
| Sim. |

|  |
| --- |
| Neste tópico, indique se os dados são reais, atualizados e se o portador consegue alterar caso precise. |
| * 1. **Qualidade dos dados** |
| *Os dados são precisos, claros e atualizados?* |
|  |
| *O portador do dado pode pedir sua correção?* |
|  |

|  |
| --- |
| Nessa etapa, vale validar com a sua equipe de TI como estão a segurança dos dados e se existe medidas de segurança, como backups, senhas de acesso, etc. |
| * 1. **Segurança e Prevenção** |
| *As medidas técnicas de segurança cabíveis estão aplicadas?* |
|  |
| *Existem medidas administrativas eficazes para proteção dos dados?* |
|  |
| *Quais as medidas adotadas para evitar danos aos titulares?* |
|  |
| *É possível comprovar medidas eficazes quanto ao cumprimento da lei? (Detalhar como)* |
| Indique aqui quais medidas são aplicadas para a segurança dos dados e qual é o nível de eficiência dessa segurança. |

|  |  |  |
| --- | --- | --- |
| **Medidas** | **Nível de eficiência** | **Aplicável a dados** |
| **Para preenchimento de FAA o usuário necessita fazer autenticação** | Alta | Sim |
| Dados anonimizados | Alta | Sim |
|  |  |  |

|  |
| --- |
| Os portadores dos dados devem ter transparência quanto aos dados, se são de fácil acesso, etc. |
| * 1. **Transparência** |
| *As informações acima estão disponíveis de forma clara e transparente para os titulares?* |
|  |

|  |  |  |
| --- | --- | --- |
| Ao final, você específica todos os riscos identificados e que posteriormente irão se tornar um plano de ação, onde o responsável pela aprovação e levantamento irão acompanhar a implementação. É importante elencar o nível dos riscos encontrados para montar uma matriz de prioridade. | | |
| 1. **Riscos identificados** | | |
| **Risco** | **Impacto** | **Probabilidade** |
| Perda da ficha de atendimento ambulatorial | Médio | Média |
| Sobreposição de dados do titular | Alto | Médio |
| Abertura de uma requisição de exame para o paciente errado | Alto | Médio |
| Medicamento aplicado a paciente alérgico | Alto | Baixo |
| Falha de comunicação dispositivo (IOT) internet | Alto | Médio |
| Dispositivo IoT danificado ou com falha de operação | Alto | Baixo |
| Impossibilidade dos servidores | Alto | Médio |
| Equipamento perdido/furtado | Alto | Baixo |
| Invasão por criptografia e resgate ao equipamento Iot | Alto | Médio |
| Equipamento sobre interferência de outros equipamentos eletrônicos | Médio | Médio |
| Indisponibilidade dos servidores em Cloud | Alto | Médio |
| Vazamento de dados transfronteiriços | Alto | Médio |
| Vazamento de dados por funcionários | Alto | Médio |
| Eventos climáticos que causem danos no ambiente do hospital | Alto | Médio |

|  |
| --- |
| **Sugestão final**  Após identificar os riscos em cada área da sua empresa, reúna os principais responsáveis para elaborar a sua Matriz de Riscos e identificar quais merecem prioridade no processo de adequação. |