LGPD | FASE-4: GOVERNANÇA | JORNADA DE ADEQUAÇÃO | SGPD | SISTEMA DE GESTÃO DE PROTEÇÃO DE DADOS

PUBLICADO EM 03/01/2020 POR PALESTRANTEMONACO

Nossos mantras

Para o entendimento dos valores profissionais que nos direcionam no dia-a-dia, declaramos os nossos principais mantras:

- “O que não é medido não é gerenciado” – Robert Kaplan.
- “Não se gerencia o que não se mede, não se mede o que não se define, não se define o que não se entende, não há sucesso no que não se gerencia” – Willian E. Deming.
- “Se você não mede algo, você não pode entender o processo. Se você não entende o processo, você não consegue aperfeiçoá-lo” – Peter Drucker.

A partir dos mantras acima declarados, foi consolidada nos últimos anos uma metodologia para a materialização de Indicadores Operacionais nomeada como Monitoração Integrada, estruturada em sete pilares de sustentação a saber:

- **AUTOMAÇÃO:** materialização de atividades operacionais automatizadas, restritas ao atual parque de tecnologia e soluções implementadas na infraestrutura de TI;
- **INCIDENTES-CLIENTES:** materialização de todas as reclamações e problemas identificados pelos usuários e/ou clientes, através de uma Central de Serviços Compartilhados (Helpdesk, Servicedesk);
- **INCIDENTES-MONITORAÇÃO:** materialização de todos os Alarmes de Monitoração configurados no ambiente, através da abertura de chamados automaticamente na Solução de Central de Serviços, gerando um Baseline de comportamento dos elementos da infraestrutura de TI e não TI;
- **OPERAÇÃO:** materialização de todas as Atividades Operacionais do dia-a-dia, que dão sustentação a manutenção da infraestrutura de TI Corporativa, através da abertura de Chamados para as equipes operacionais e de manutenção;
- **REQUISIÇÕES:** materialização de todas as solicitações demandas pelos usuários / clientes, com via Catálogos de Serviços disponibilizados à partir de uma Central de Serviços Compartilhados (Helpdesk, Servicedesk);
- **SUPORTE TÉCNICO:** materialização de todas as Atividades de Suporte Técnico, que dão sustentação a manutenção da infraestrutura de TI Corporativa da CONTRATANTE, através da abertura de Chamados para as equipes operacionais e de manutenção;

- **MELHORIA CONTÍNUA:** materialização de todas as atividades de Melhoria Contínua executadas pela equipe técnica de TI.

Um contexto corporativo foi consolidado nestes anos de uso efetivo da Monitoração Integrada em função dos investimentos, custos e esforços envolvidos nas atividades de sustentação do dia-a-dia:

PROCESSOS	40%
PESSOAS	40%
TECNOLOGIA	20%

LGPD – Lei Geral de Proteção de Dados

Dentre os principais posicionamentos corporativos no mercado nacional frente às necessidades de adequação à LGPD destacam-se:

- “No Brasil, as datas não são cumpridas e a nova legislação de Proteção de Dados não entrará em vigor em Agosto/2020”.
- “A nova legislação não vai nos impactar”.
- Precisamos identificar e nomear imediatamente quem será o responsável interno por se posicionar no mercado, com relação a nova legislação”.
- “Já estou atuando no contexto de adequação à nova legislação, pois já estou tratando com o meu parceiro de tecnologia a identificação dos investimento na aquisição de ferramentas específicas”.
- Dentre outros…..

Em função dos posicionamentos acima declarados, nos deparamos com a seguinte situação real:

- Grande probabilidade da LGPD entrar em vigor em 2020.
- Todas as empresas serão impactadas uma vez que:
  - **Gerenciamento de Colaboradores**: 100% Dados Pessoais e/ou Dados Pessoais Sensíveis são tratados pelos Departamentos Pessoais ou Recursos Humanos nas empresas;
  - **Folha de Pagamento**: mais de 60% das empresas tem Sistema de Folha de Pagamento terceirizado e/ou contratado em uma modalidade SaaS (‘Software as a Service) na Nuvem;
  - **Discrepância de informações sobre o domínio direto de Recursos Humanos e da Tecnologia:** mais de 50% das empresas tem um

Processo de Gerenciamento de Acesso a Infraestrutura de Tecnologia "quebrado", uma vez que, a manutenção da situação atual dos colaboradores não é 100% replicada entre estes departamentos corporativos;

- **Ambiente Corporativo complexo e distribuído** trazendo um grande desafio ao gerenciamento do armazenamento e da manipulação dos Dados Pessoais, além do desafio inerente ao gerenciamento de Incidentes de Segurança da Informação e Vazamento de Dados Corporativos.

Outro posicionamento de Mercado bastante **comum relacionado a LGPD**:

- "Eu entendo que, por se tratar de uma nova Legislação, e darei foco em contratar um Advogado para me direcionar no contexto".

A jornada de adequação corporativa à LGPD demanda de um forte direcionamento de Governança Corporativa para se identificar o **"onde" os Dados Pessoais são utilizados no dia a dia-a-dia** e somente à partir de então, direcionar esforços na sustentação da Legislação, de Contratos e Normas Regulatórias, de forma que um conjunto de ações específicas não são inerentes ao perfil de um Advogado, como por exemplo:

- Mapeamento de Processos de Negócios;
- Mapeamento de todas as Aplicações utilizadas;
- Mapeamento dos Fluxos de Dados Pessoais: Físicos | Digitais;
- Mapeamento do Inventário dos Dados Pessoais: Físicos | Digitais;
- Classificação dos Dados Pessoais: independentemente do meio – Físicos | Digitais;
- Análise de Impacto da Privacidade de Dados Pessoais: Físicos | Digitais;
- Estrutura Organizacional para a Governança de Dados Pessoais*;*
- Aspectos da Segurança da Informação, e;
- Melhores Práticas: ITIL, COBIT, Gestão de Projetos, ISO 27.001, etc.

Proposta Wellington Monaco

Em função das experiências acumuladas na utilização efetiva da metodologia de Monitoração Integrada dentro de um contexto corporativo de Centrais de Serviços Compartilhados, e perante o desafio de adequação à LGPD, novos conhecimentos e estudos foram necessários via **Certificação DPO | Data Protection Officer | EXIN.**

Nesta jornada de estudos e entendimento da evolução para a consolidação da Legislação de Privacidade de Dados na Europa – Área Econômica Europeia (AEE) nomeada como **GDPR (General Data Protection Regulation)**, abaixo exemplificada;

consolidou-se um **Framework, um Sistema, uma "JORNADA" estruturada** para a adequação corporativa à Legislação de Privacidade de Dados Pessoais.

Sistema de Gestão de Proteção de Dados – SGPD

O objetivo de um Framework, de um **Sistema de Gestão de Proteção de Dados – SGPD** é estruturar um processo responsável pelo gerenciamento e por mitigar os riscos de proteção de dados e privacidade envolvidos em todo o **Ciclo de Vida de Dados Pessoais** no ambiente corporativo, considerando-se desde a coleta, o processamento e a eliminação de dados pessoais.

O Sistema proposto de **Proteção de Dados e Privacidade** inclui uma metodologia consolidada em processos, fases, etapas, políticas, procedimentos e várias ferramentas técnicas.

Fase-4: Governança de Proteção de Dados e Privacidade

O principal objetivo desta fase considerada dentro do sistema proposto, é desenvolver e implementar medidas e controles específicos de Proteção e Privacidade de Dados considerando-se:

- estruturas de organizacionais específicas através de um programa de Proteção de Dados e Privacidade, com a nomeação de um Responsável (pessoa física) e um Comitê de Proteção e Privacidade,
- “modus operandus” para o contínuo envolvimento e comprometimento todas as partes envolvidas com a Proteção de Dados e Privacidade, e:
- relatar continuamente todos os problemas de privacidade e proteção de dados.
- projetar um sistema de classificação de dados;
- desenvolver e implementar políticas, procedimentos e controles para adequação corporativa às leis e requisitos de proteção de dados e privacidade

Esta fase é composta por:

- **7 Etapas**
- **9 Resultados previstos**

Com relação às **7 (sete) etapas consideradas nesta Fase-4: Governança de PD&P**, temos:

- **Etapa #1:** Implementar práticas de Gerenciamento do Uso de Dados Pessoais.
- **Etapa #2:** Manter devidamente atualizados todos os avisos de Privacidade de Dados.
- **Etapa #3:** Executar um Plano de Solicitações, Reclamações e Retificação.
- **Etapa #4:** Executar uma Avaliação de Risco sobre a Proteção de Dados (AIPD).
- **Etapa #5:** Emitir Relatórios (Internos e Externos) de Proteção de Dados e Privacidade
- **Etapa #6:** Manter a documentação de Privacidade de Dados devidamente atualizada

- **Etapa #7:** Estabelecer e manter um plano de resposta à violação de privacidade de dados

Etapa #1: Implementar práticas de Gerenciamento do Uso de Dados Pessoais.

Esta etapa é responsável por implementar políticas e procedimentos específicos para a coleta, uso e eliminação de dados pessoais e dados pessoais sensíveis.

Dados sensíveis

Alguns tipos de dados pessoais são classificados como sensíveis e requerem considerações adicionais quanto a gestão e proteção.

Exemplos comuns do que geralmente se é considerado como **"dado sensível"** incluem: opiniões políticas, origem racial ou étnica; dados relacionados à vida sexual; crenças religiosas ou filosóficas; filiação a um sindicato; informações de saúde física ou mental, bem-estar social; informação financeira; identificadores governamentais como por exemplo números de seguridade social; acusações criminais ou condenações; biometria; dados genéticos; dados de localização; e Dados referentes a crianças.

Uma prática bastante comum às empresas são as práticas, políticas e procedimentos para coleta e uso de dados pessoais sensíveis no seu dia-a-dia, incluindo dados biométricos, dados de crianças, etc.

O Responsável pela Proteção de Dados e Privacidade deve garantir que estas práticas sejam implementadas na cultura organizacional para adicionar medidas de proteção necessárias para se garantir a legalidade do processamento de dados pessoais sensíveis.

Processo automatizado de tomada de decisão para dados pessoais

As empresas devem introduzir um processo manual de revisão das decisões automatizadas que impactam diretamente os indivíduos.

O Responsável pela Proteção de Dados e Privacidade deve garantir que essas práticas sejam implementadas na sua totalidade para se evitar os riscos potenciais da tomada de decisão automatizada sobre esses dados pessoais.

Usos secundários de dados pessoais

Empresas devem implementar práticas, políticas e procedimentos que definem e sustentam o objetivo do processamento de dados pessoais, assim como lidar com as situações em que deseja usar os dados pessoais de maneiras diferentes das finalidades previamente definidas.

O Responsável pela Proteção de Dados e Privacidade garante que essas práticas sejam implementadas em sua totalidade para se evitar os riscos potenciais de processamento secundário não autorizado de dados pessoais.

- **Resultado previsto – Etapa #1:**
  - **Estratégia atualizada de Proteção de Dados e Privacidade**
  - **Política de Proteção de Dados**

Etapa #2: Manter avisos de Privacidade sobre os Dados Pessoais

As empresas devem implementar **avisos e rastreio** de privacidade de dados para o contínuo posicionamento dos Titulares de acordo com a Política de Privacidade de Dados, requisitos legais e tolerância a riscos operacionais considerando-se:

- quais dados pessoais são coletados;
- como os dados pessoais são coletados, usados, mantidos, retidos, divulgados, eliminados, e;
- que controle específico têm os Titulares dos dados pessoais envolvidos.

Especificamente para os pontos em que a empresa coleta dados pessoais – online, mensagens de texto, telefone, pessoalmente, comunicações de marketing, formulários de solicitação de funcionários – algumas considerações são relevantes:

- o Titular em questão tem a oportunidade de **revisar o aviso de privacidade de dados ou receber informações sobre as práticas de privacidade de dados da empresa**, antes de fornecer seus dados pessoais (aviso “just in time”);
- a empresa fornece **informações simplificadas** relacionadas às suas políticas e práticas de privacidade ao público, por meios visuais, por e-mails, folhetos, ofertas, pôsteres e placas;
- a empresa fornece avisos sobre as **solicitações de serviços, recebimentos, faturas, contratos e termos de serviços** dos Titulares;

- mediante a **coleta de dados pessoais** via telefone ou pessoalmente, a empresa fornece **instruções orientadoras para uso dos funcionários da linha de frente de atendimento aos Titulares**, para fornecer explicações

básicas das políticas e práticas de privacidade corporativa, incluindo a coleta e o uso dos dados pessoais coletados;

- quanto a **emissão de avisos de privacidade no site corporativo na internet**, a empresa garante que os selos ou marcas de confiabilidade sejam exibidos no(s) site(s) da empresa, para garantir aos visitantes do site a legitimidade do site e demonstrar um compromisso com os princípios de privacidade definidos por um terceiro (o fornecedor do selo ou marca de confiança).
- **Resultado previsto – Etapa #2:**
    - **Procedimento para manutenção de Avisos de Privacidade de Dados**

Etapa #3: Executar um Plano de Solicitações, Reclamações e Retificação

Etapa é responsável pela execução das atividades relacionadas ao tratamento de reclamações, gerenciando solicitações de acesso e atualização de informações pelos indivíduos de seus dados pessoais mantidos pela empresa, definidos na Fase-3: Definição e Implementação.

Neste Plano de Solicitações, Reclamações e Retificações considera-se:

- Procedimentos de Acesso a Dados Pessoais;
- Procedimentos de Reclamações de Dados Pessoais;
- Procedimentos de Retificação de Dados Pessoais;
- Procedimentos de Objeção de dados pessoais;
- Procedimentos de Portabilidade de Dados Pessoais;
- Procedimentos de Eliminação de Dados Pessoais e;
- Procedimentos de Rastreabilidade sobre Manipulação de Dados Pessoais.

Na GDPR – Artigo 12 – Controlador tem o prazo de 1 (um) mês para atender às solicitações dos Titulares.

No caso da LGPD este procedimento demanda de instruções específicas a ANPD – Agência Nacional de Proteção de Dados.

- **Resultado previsto – Etapa #3:**
    - **Estrutura de Solicitações, Reclamações e Plano de Retificação**

Etapa #4: Executar uma Avaliação de Riscos sobre a Proteção de Dados (AIPD)

Etapa responsável pela realização de três atividades principais:

- Avaliação de Riscos de Proteção de Dados
- Riscos de Terceiros
- Avaliação de Riscos de Privacidade e negócios

Avaliação de Riscos de Proteção de Dados

- O escopo do **Programa de Proteção de Dados e Privacidade** é determinado pelos desafios de conformidade legal e regulamentar e pelos dados pessoais diretamente envolvidos, consolidados durante a Fase-1: Preparação, e devidamente atualizado na Fase-2:Organização e na Fase-3:Definição e Implementação.
- Implementação do **Processo de Avaliação de Riscos de Proteção de Dados** como pré-requisito para um efetivo Programa corporativo de Proteção de Dados e Privacidade, através do qual a estrutura organizacional responsável – Escritório de Proteção e Dados e Privacidade – define, implementa e executa contínuas e periódicas avaliações de Riscos de Proteção de Dados, de privacidade e de segurança da informação nas unidades de negócios, nos processos de negócios, nas comunicações e nos treinamentos corporativos, etc.
- O principal objetivo do processo de **Avaliação de Riscos de Proteção de Dados** é se identificar e priorizar as lacunas de Privacidade de Dados e Segurança da Informação em toda a organização, e gerenciar efetivamente o Programa de Privacidade de Dados para a **mitigação de riscos, manutenção da conformidade, aumentar a reputação da marca e a confiança da empresa**.

Riscos de terceiros

- A estrutura organizacional responsável pela Proteção de Dados e Privacidade – Escritório de Proteção e Dados e Privacidade – também garante que os riscos de terceiros sejam gerenciados adequadamente.

Avaliação de Riscos de Privacidade e Negócios

- Considerar dentro das atuais funções corporativas de Gerenciamento de Riscos do Negócio – identificar e avaliar os fatores e problemas que podem afetar o sucesso de suas operações comerciais – o envolvimento da estrutura de Escritório de Proteção de Dados e Privacidade para incorporar os aspectos de Gerenciamento de Riscos de Privacidade que possam afetar os esforços de negócios da empresa.
- A **Análise e Avaliação de Riscos sobre Proteção de Dados e Privacidade** apenas aborda como os riscos de dados podem ser avaliados, não considerando todos os métodos para revisar riscos e mitigar controles, nem lista todos os riscos que surgirão em uma avaliação de riscos de negócios.

No **caso da GDPR Europeia** existem especificações detalhadas sobre as situações em que é obrigatória uma Avaliação de Riscos sobre a Proteção de Dados (AIPD).

Já no contexto da LGPD, a obrigatoriedade sobre a execução de uma Avaliação de Riscos sobre a Proteção de Dados (AIPD) ainda não foi declarada pela ANPD (Agência Nacional de Privacidade de Dados).

- **Resultado previsto – Etapa #4:**
    - **Estrutura de Solicitações, Reclamações e Plano de Retificação**

Etapa #5: Emitir Relatórios (Internos e Externos) de Proteção de Dados e Privacidade

Etapa responsável pela geração de Relatórios Internos (Conselho de Administração, Diretorias, Gerências e Acionistas) e Relatórios Externos (órgãos reguladores, terceiros, parceiros e clientes).

Relatório para partes interessadas internas sobre o status da Proteção de Dados e do Gerenciamento de Privacidade:

- **Interessados:** Conselho de Administração, Executivos Seniores, Diretoria, Gerência e Acionistas;
- **Objetivos:**
    - informar de maneira contínua, periódica, precisa, abrangente e eficiente aos responsáveis pela supervisão e gerenciamento do Programa de Proteção de Dados e Privacidade de dados, para garantir os esforços e investimentos necessários para que a empresa atinja a conformidade e reduza os riscos relacionados ao processamento de dados pessoais;
    - contínuo e periódico alinhamento da função de Proteção de Dados e Privacidade com os objetivos estratégicos da empresa, concentrando-se em como a privacidade suporta os resultados da organização, além de destacar o status de conformidade com os requisitos legais e regulamentares.

Relatório para partes interessadas externas sobre o status da Proteção de Dados e do

- **Interessados** Gerenciamento de Privacidade:**:** Órgãos Reguladores, terceiros, parceiros, fornecedores e clientes
- **Objetivos:**
    - criar transparência e confiança entre clientes, terceiros, fornecedores, Órgãos Reguladores de Proteção de Dados e Privacidade e o público em geral.
- **Resultado previsto – Etapa #5:**
    - **Relatórios (Interno e Externo) de Proteção de Dados e Privacidade.**

Etapa #6: Manter a documentação de Privacidade de Dados devidamente atualizada

Etapa responsável pela manutenção de toda a documentação que reflete o status atualizada do Programa de Proteção de Dados e Privacidade, devidamente atualizada uma vez que, pode ser requisitada pelo Órgão Regulador – ANPD – Agência Nacional de Privacidade dos Dados., para a verificar a conformidade legal.

Essa documentação também serve como evidência ao solicitar 'marcas de confiança', selos, "BCR" (Binding Corporate Rules) ou Regras Corporativas Vinculantes, certificações e participação em outros programas de auto regulação.

- **Resultado previsto – Etapa #6:**
    - **Processo de manutenção da Documentação de Privacidade de Dados.**

Etapa #7: Estabelecer e manter um plano de resposta à violação de privacidade de dados

Esta etapa é responsável por projetar, desenvolver, implementar e manter um efetivo Plano de Resposta a Incidentes de Segurança ou Plano de Violação de Privacidade de Dados capaz de fornecer uma forma coerente, sistemática e proativa de se Gerenciar Violações de Privacidade de Dados e Gerenciar Incidentes de Segurança que afetam os dados pessoais de maneira consistente.

Dentre as funções consideradas para um Plano de Resposta a Incidentes de Segurança ou Plano de Violação de Privacidade de Dados temos:

- a operacionalização de um procedimento de **notificação de violação** aos Titulares afetados;
- a necessidade de se relatar todos os **Incidentes ou Violações de Privacidade de Dados** aos Órgãos Reguladores, agência governamentais, agências de crédito, autoridades policiais e outros terceiros externos em tempo um **tempo legalmente definido**;
- a necessidade de se manter todos os **registros referentes a detalhes** sobre Incidentes ou Violações de Privacidade de Dados com o objetivo de alcançar a conformidade legal e normas regulatórias de setores específicos;
- de garantir que as notificações e relatórios de violação de privacidade de dados estejam alinhados com os requisitos legais e as melhores práticas;
- que monitorar, documentar e relatar incidentes de privacidade de dados ou métricas de violação, para que a eficácia das políticas e procedimentos de resposta a violação de dados seja avaliada e validada;
- realizar testes contínuos e periódicos quanto ao Plano de Resposta à Violação de Privacidade e Plano de Resposta a Incidentes de Segurança, e;

- contratar cobertura adequada de seguro de Violação de Privacidade de Dados para os custos associados a uma violação de privacidade.
- **Resultado previsto – Etapa #7:**
    - **lano de Resposta à Violação de Privacidade de Dados.**

Resultados – Fase-4: Governança

Dentre as 7 (sete) etapas acima consideradas, os **seguintes resultados são previstos Fase-4: Governança** dentro do Sistema de Gestão de Privacidade de Dados proposto:

- **Estratégia atualizada de Proteção de Dados e Privacidade – Etapa #1;**
- **Política de Proteção de Dados – etapa #1;**
- **Procedimento para Manutenção de Avisos de Privacidade de Dados – Etapa #2;**
- **Estrutura de Solicitações, Reclamações e Plano de Retificação – Etapa #3;**
- **Processo de Avaliação de Riscos sobre Proteção de Dados – Etapa #4;**
- **Plano de Gerenciamento de Riscos de Terceiros – Etapa #4;**
- **Relatórios (Interno e Externo) de Proteção de Dados e Privacidade – Etapa #5;**
- **Processo de manutenção da Documentação de Privacidade de Dados – Etapa #6;**
- **Plano de Resposta à Violação de Privacidade de Dados – Etapa #7.**

O resultado efetivo da Fase-4: Governança é estabelecer as estruturas organizacionais de Governança para melhorar continuamente a Proteção dos Dados e o Gerenciamento da Privacidade.