# LGPD | VISÃO GERAL | JORNADA DE ADEQUAÇÃO | SISTEMA DE GESTÃO DE PROTEÇÃO DE DADOS

**PUBLICADO EM 27/12/2019 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.


# 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-1: Preparação

O principal objetivo desta fase considerada dentro do sistema proposto, é a consolidação de um ambiente corporativo “preparado” para a Proteção e Privacidade dos Dados Pessoais, considerando-se os processos corporativos mapeados e consolidados, os requisitos técnicos e operacionais da proteção de dados e a privacidade, que afetam sua empresa.


**Esta fase é composta por:**

- **8 Etapas**
- **10 Resultados previstos**

Com relação às **8 (oito) etapas consideradas nesta Fase-1**, temos:

- **Etapa #1:** Realizar a Análise de Privacidade
- **Etapa #2:** Coletar Leis de Privacidade
- **Etapa #3:** Analisar o impacto da Privacidade no negócio
- **Etapa #4:** Realizar Auditorias e Avaliações dos dados iniciais
- **Etapa #5:** Estabelecer a estrutura organizacional de Governança de Dados
- **Etapa #6:** Estabelecer Fluxo de Dados e Inventário de Dados Pessoais
- **Etapa #7:** Estabelecer programa de Proteção de Dados e Privacidade
- **Etapa #8:** Esboçar Planos de Implementação de ações de Proteção de Dados e Privacidade

E dentre as 8 (oito) etapas consideradas, teremos os seguintes **resultados previstos:**

1. **Relatório de Análises de Proteção de Dados e Privacidade – Etapa #1**
2. **Manual de Leis de Privacidade – Etapa #2 e #3**
3. **Relatório de Auditoria de Dados Pessoais – Etapa #4**
4. **Sistema de Fluxo de Dados por Processo – Etapa #6**
5. **Inventário de Dados Pessoais – Etapa #6**
6. **Política de Proteção de Dados – Etapa #6**
7. **Plano de Treinamento em Privacidade – Etapa #7**
8. **Programa de Proteção de Dados & Privacidade – Etapa #7**
9. **Orçamento da estruturação da Gestão de Proteção de Dados – Etapas #1 a #8**
10. **Planos de Implementação de Ações de Proteção de Dados e Privacidade – Etapas #1 à #8**

**Resultado final:** Uma organização preparada para ser eficiente no tratamento e gerenciamento dos riscos envolvidos na Proteção de Dados e Privacidade.

# Fase-2: Organização

O principal objetivo desta fase considerada dentro do sistema proposto, é a estabelecer as estruturas e mecanismos organizacionais responsáveis por atender às necessidades de privacidade de dados pessoais da empresa, considerando.se:

- desenhar e implementar o programa de proteção de dados e privacidade;
- designar um Encarregado de Dados – pessoa física;
- engajar e comprometer todas as partes envolvidas com a proteção de dados e privacidade, e;
- estabelecer as estruturas organizacionais adequadas para uma efetiva proteção de dados e implementação de privacidade.


**Esta fase é composta por:**

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

Com relação às 7 (sete) etapas consideradas nesta Fase-1, temos:

- **Etapa #1:** Definir e implementar o “como manter” o programa, as políticas e controles de Governança de Privacidade de Dados.
- **Etapa #2:** Definir e manter a matriz de atribuições e responsabilidades pela Proteção de Dados e Privacidade – Matriz RACI.
- **Etapa #3:** Definir e implementar o “como manter” o envolvimento dos níveis táticos e estratégicos da organização – Gerência Senior – na Proteção de Dados e Privacidade.
- **Etapa #4:** Estabelecer e manter a continuidade do compromisso de todos os níveis hierárquicos da organização com a Proteção de Dados e Privacidade – PD&P.
- **Etapa #5:** Estabelecer e manter um plano de comunicação corporativa regular para direcionamentos, questões e problemas de Proteção de Dados e Privacidade.
- **Etapa #6:** Estabelecer e manter processos e procedimentos que garantam o envolvimento das partes interessadas em questões de Proteção de Dados e Privacidade.
- **Etapa #7:** Implementar e operar sistemas informatizados para a sustentação da Proteção de Dados e Privacidade corporativa.

E dentre as 7 (sete) etapas consideradas, teremos os seguintes **resultados previstos:**

1. **Estratégia de Proteção de Dados e Privacidade atualizada – Etapa #1.**
2. **Programa de Proteção de Dados e Privacidade atualizado – Etapa #1.**

3. **Controles de Governança de Dados atualizados – Etapa#1.**
4. **Nomeação do Encarregado da Proteção de Dados Pessoais – pessoa física – Etapa #2.**
5. **Plano de Comunicação para todas questões de PD&P – Etapas #3, #4, #5 e #6.**
6. **Rede corporativa de PD&P – Etapa #4.**
7. **Função de Proteção de Dados e Privacidade incluída nas descrições de cargos – Etapa#4.**
8. **Plano atualizado de conscientização, comunicação e treinamento em privacidade – Etapa #5.**
9. **Sistema informatizado de Proteção de Dados e Privacidade – Etapa #7.**

**Resultado final:** Estruturas organizacionais aderentes à implementação da Proteção de Dados e Privacidade.

# Fase-3: Desenvolvimento e Implementação

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

- projetar um Sistema de Classificação de Dados;
- desenvolver e implementar políticas, procedimentos e controles para cumprir a Legislação de Privacidade e requisitos da Organização.


Esta fase é composta por:

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

Com relação às **7 (sete) etapas** consideradas nesta Fase-1, temos:

- **Etapa #1:** Definir e implementar o “como manter” o programa, as políticas e controles de Governança de Privacidade de Dados.
- **Etapa #2:** Definir e manter a matriz de atribuições e responsabilidades pela Proteção de Dados e Privacidade – Matriz RACI.

- **Etapa #3:** Definir e implementar o “como manter” o envolvimento dos níveis táticos e estratégicos da organização – Gerência Senior – na Proteção de Dados e Privacidade.
- **Etapa #4:** Estabelecer e manter a continuidade do compromisso de todos os níveis hierárquicos da organização com a Proteção de Dados e Privacidade – PD&P.
- **Etapa #5:** Estabelecer e manter um plano de comunicação corporativa regular para direcionamentos, questões e problemas de Proteção de Dados e Privacidade.
- **Etapa #6:** Estabelecer e manter processos e procedimentos que garantam o envolvimento das partes interessadas em questões de Proteção de Dados e Privacidade.
- **Etapa #7:** Implementar e operar sistemas informatizados para a sustentação da Proteção de Dados e Privacidade corporativa.

E dentre as 7 (sete) etapas consideradas, teremos os seguintes **resultados previstos:**

1. **Sistema de Classificação de Dados Pessoais – Etapa #1**
2. **Procedimento de aprovação do Processamento dos Dados Pessoais – Etapa #2.**
3. **Documento de Registro dos Bancos de Dados que contém Dados Pessoais – Etapa #3**
4. **Desenvolvimento e implementação de um Sistema de transferência internacional de Dados – Etapa #4**
5. **Atividades de Integração de Proteção de Dados e Privacidade executadas – Etapa #5**
6. **Atividades de treinamento corporativo de Proteção de Dados e Privacidade executadas – Etapa #6**
7. **Controles de Segurança de Dados Pessoais implementados – Etapa #7**

**Resultado final:** Desenvolver e implementar um conjunto de medidas de Proteção e Privacidade para administrar os dados pessoais de maneira eficiente e eficaz.

# Fase-4: Governança

O principal objetivo desta fase considerada dentro do sistema proposto é estabelecer mecanismos de Governança de Privacidade dos Dados Pessoais, considerando-se:

- desenhar e configurar estruturas organizacionais de Governança no contexto de Proteção de Dados e Privacidade;
- envolver e obter o comprometimento de todas as partes interessadas relevantes;

- relatar todas as questões de Privacidade considerando-se um contexto de processo contínuo.


**Esta fase é composta por:**

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

Com relação às **7 (sete) etapas consideradas nesta Fase-4**, temos:

- **Etapa #1:** Implementar práticas Governança para o gerenciamento do uso dos Dados Pessoais ao longo de todo o Ciclo de Vida.
- **Etapa #2:** Manter avisos de Privacidades sobre os Dados Pessoais.
- **Etapa #3**: Executar um plano de solicitações, reclamações e retificações.
- **Etapa #4**: Executar uma Avaliação de riscos de Proteção de Dados – Análise de Impacto a Proteção de Dados – AIPD.
- **Etapa #5:** Emitir Relatório de Proteção de Dados e Privacidade.
- **Etapa #6:** Manter documentação de Privacidade de Dados.
- **Etapa #7:** Estabelecer e manter um Plano de Resposta de Violação de Privacidade.

E dentre as 7 (sete) etapas consideradas, teremos os seguintes **resultados previstos:**

1. **Estratégia de Proteção de Dados e Privacidade atualizada – Etapa #1.**
2. **Política de Proteção de Dados – Etapa #1.**
3. **Procedimentos para manter Avisos de Privacidade de Dados – Etapa #2.**
4. **Plano de tratamento de solicitações, reclamações e retificação – Etapa #3.**
5. **Processo de Avaliação de Riscos para Proteção de Dados – Etapa #4.**
6. **Plano de Gerenciamento de Riscos de Terceiros – Etapa #4.**
7. **Relatório de Proteção de Dados & Privacidade – Etapa #5.**
8. **Documentação de Privacidade de Dados – Etapa #6.**
9. **Plano de Resposta à Violação de Privacidade de Dados – Etapa #7**

**Resultado final:** Estabelecer uma estrutura de Proteção de Dados e Governança da Privacidade para uma melhor proteção dos dados e gerenciamento de privacidade.

# Fase-5: Avaliação e melhoria

O principal objetivo desta fase considerada dentro do sistema proposto é avaliar, monitorar e melhorar continuamente todos os aspectos específicos de Proteção de Dados e Privacidade da Organização (controles, políticas, procedimentos, práticas, etc.), considerando-se:

- monitorar a operação e a resolução de todas as questões relacionadas à Privacidade;
- avaliar regularmente a conformidade dos processos e políticas internas, e;
- melhorar a Proteção de Dados e as medidas de Privacidade.


**Esta fase é composta por:**

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

Com relação às **7 (sete) etapas consideradas nesta Fase-4**, temos:

- Etapa #1: Realizar auditoria interna de PD & P
- Etapa #2: Envolver uma parte externa para avaliações de PD & P.
- Etapa #3: Realizar avaliações e estabelecer “benchmarkes” (comparações).
- tapa #4: Executar avaliações de riscos de Proteção de Dados.
- Etapa #5: Resolver riscos de PD & P.
- Etapa #6: Relatar análise de riscos de PD & P e resultados
- Etapa #7: Monitorar as leis e regulamentos de PD

E dentre as 7 (sete) etapas consideradas, teremos os seguintes **resultados previstos:**

1. **Relatório de auditoria interna sobre PD & P – Etapa #1.**
2. **Relatório de auditoria externa sobre PD & P – Etapa #2.**
3. **Relatório de Avaliação de Privacidade ad-hoc – Etapa #3.**
4. **Relatório de autoavaliação de Privacidade – Etapa #3.**
5. **Relatório de benchmark (comparação) de Privacidade – Etapa #3**
6. **Relatório de Avaliação de Impacto sobre a Proteção de Dados – AIPD – Etapa #4.**
7. **Relatório de riscos tratados para PD & P – Etapa #5.**
8. **Relatório de Análise de Riscos e Resultados de PD & P – Etapa #6.**
9. **Relatório de Monitoramento da Legislação envolvida na Privacidade de Dados Pessoais – Etapa #7.**

**Resultado final:** Monitoração e auditaria contínua dos aspectos de Proteção e Privacidade de Dados para a identificação de falhas e pontos de melhorias nos atuais procedimentos e controles implementados, incluindo um plano de ação para a melhoria contínua da Política e Programa de Proteção e Privacidade de Dados Pessoais.