LGPD | FASE-3: DEFINIÇÃO E IMPLEMENTAÇÃO | JORNADA DE ADEQUAÇÃO | SGPD | SISTEMA DE GESTÃO DE PROTEÇÃO DE DADOS

PUBLICADO EM 31/12/2019 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.

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

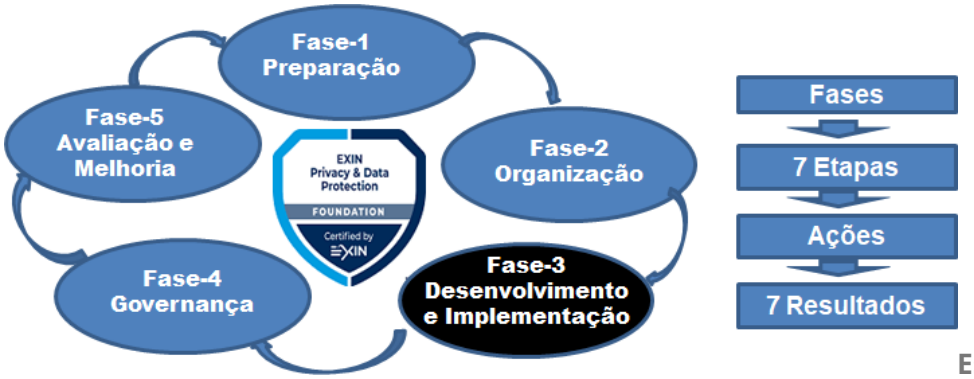
O objetivo de um Framework, de um **Sistema de Gestão de Proteção de Dados – SGPD** é estruturar um processo responsável pelo gerenciamento e por mitigar os riscos de proteção de dados e privacidade envolvidos em todo o **Ciclo de Vida de Dados Pessoais** no ambiente corporativo, considerando-se desde 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-3: Desenvolvimento e Implementação

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:

- 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**
- **7 Resultados previstos**

Com relação às **7 (sete) etapas consideradas nesta Fase-3**, temos:

- **Etapa #1:** Desenvolver e implementar estratégias, planos e políticas de Proteção de Dados e Privacidade.
- **Etapa #2:** Implementar procedimento específico para aprovação do processamento de dados pessoais (Ciclo de Vida).
- **Etapa #3:** Registrar bancos de dados que contenham dados pessoais.
- **Etapa #4:** Desenvolver e implementar um sistema para a transferência internacional de dados pessoais (caso necessário).
- **Etapa #5:** Executar atividades de integração da gestão de Dados Pessoais e Privacidade no dia-a-dia corporativo
- **Etapa #6:** Executar plano de treinamento específico da Política Corporativa de Dados Pessoais e Privacidade.
- **Etapa #7:** Implementar controles de Segurança de Dados.

Etapa #1: Desenvolver e implementar estratégias, planos e políticas de Proteção de Dados e Privacidade.

Esta etapa é responsável por:

- desenvolver e implementar estratégias, planos, políticas e controles adequados:
    - a partir da consolidação dos requisitos técnicos e operacionais do negócio;
    - a partir da consolidação de uma Matriz de Responsabilidade.
- desenvolver e implementar um Sistema de Classificação de Dados Pessoais considerando-se:
    - alguns agrupamentos de dados pessoais como “disponíveis publicamente”, “confidenciais”, “sensíveis”, etc;
    - o controle e redução do escopo “do que precisa ser” e “como” deve ser protegido;
    - a criação e implementação de procedimentos para classificação de dados considerando-se detalhes sobre a propriedade de dados, requisitos de retenção, requisitos de uso e de proteção com base no nível de classificação e requisitos legais.
- **Resultado previsto:** Sistema de Classificação de Dados Pessoais.

Etapa #2: Implementar procedimento específico para aprovação do processamento de dados pessoais (Ciclo de Vida).

Esta etapa é responsável por:

- Em algumas situações as empresas e organizações devem obter aprovação dos reguladores de proteção de dados e privacidade antes de coletar e processar dados pessoais (GDPR – Artigo 36 – Consulta Prévia);
- processamento de dados pessoais sensíveis; processamento de dados pessoais com a finalidade de avaliar aspectos pessoais do indivíduo ou determinar a elegibilidade do indivíduo para um direito, benefício ou contrato; e coleta e processamento em larga escala (por exemplo, Big Data), etc.
- **Consolidar:** Procedimento para aprovação do processamento de dados pessoais.

Etapa #3: Registrar os Bancos de Dados que contenham dados pessoais.

Esta etapa é responsável por:

- Registrar junto aos reguladores de proteção de dados os Bancos de Dados Corporativos que contenham Dados Pessoais, e qual é o processamento pretendido (GDPR – Artigo 36 – Consulta Prévia).
- **Resultado previsto:** Documento de registro de Bases de Dados contendo Dados Pessoais.

Etapa #4: Desenvolver e implementar um sistema para a transferência internacional de dados pessoais (caso necessário).

Esta etapa é responsável por:

- manter uma documentação sobre todos os fluxos internacionais de dados pessoais, acompanhando seu uso e cumprimento de mecanismos de transferência transfronteiras, tais como: códigos corporativos de conduta, como **regras corporativas vinculantes (BCR)**, cláusulas contratuais, aprovações da autoridade de proteção de dados, possíveis dependências de isenção dos requisitos de transferência, conforme estabelecido na lei;
- Utilizar cláusulas modelos disponibilizadas pelos Governos e órgãos reguladores para facilitar a transferência de dados pessoais de um regime de proteção à privacidade para um destinatário em um país que não fornece proteções adequadas para dados pessoais;
- **Resultado previsto:** Sistema transferência internacional de Dados Pessoais.

Etapa #5: Executar atividades de integração da gestão de Dados Pessoais e Privacidade no dia-a-dia corporativo

Esta etapa é responsável por:

- Considerar os direcionamentos de Proteção de Dados e Privacidade em todos os aspectos estratégicos, táticos e operacionais do dia-a-dia corporativo, considerando-se:
    - retenção de registros corporativos de tratamento de dados pessoais;
    - contratação de Colaboradores, Terceiros e Parceiros;
    - acesso ao site:
    - Marketing digital;
    - Mídia social:
    - Utilização de dispositivos portáteis e inteligentes – BYOD;
    - Saúde e Segurança;
    - Desenvolvimento de Sistemas, Produtos e Processos – “Privacy by Design”.
- **Resultado previsto:** Atividades estratégicas, táticas e operacionais do dia-a-dia corporativo devidamente integradas aos direcionamentos de Proteção de Dados Pessoais e Privacidade.

Etapa #6: Executar plano de treinamento corporativo para Dados Pessoais e Privacidade

Esta etapa é responsável por:

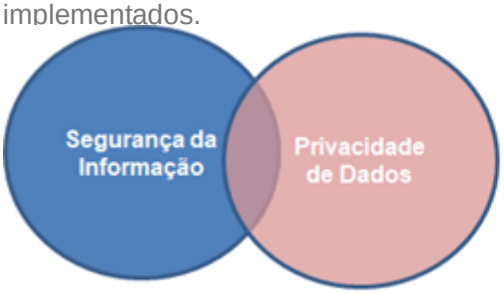
- Executar um plano contínuo de treinamento e conscientização (colaboradores, terceiros, parceiros e demais contratados) quanto aos direcionamentos de Proteção de Dados e Privacidade de Dados Pessoais envolvidos nas atividades, procedimentos, programas, sistemas, projetos e funções no dia-a-dia corporativo, considerando-se:
    - treinamento básico e contínuo de privacidade para toda a equipe;
    - treinamento adicional de privacidade para novas necessidades – “Privacy by Design”;
    - considerar aspectos de treinamento de privacidade de dados em todos os treinamentos corporativos – tema constante;
    - conscientização contínua dos aspectos de Privacidade de Dados no dia-a-dia corporativo;
- Manter a certificação profissional de privacidade de dados para o pessoal de privacidade;
- Monitorar indicadores do nível corporativo de reconhecimento, de conscientização e de treinamento dos aspectos de Privacidade de Dados.
- **Resultado previsto:** Executar plano de treinamento corporativo para Dados Pessoais e Privacidade.

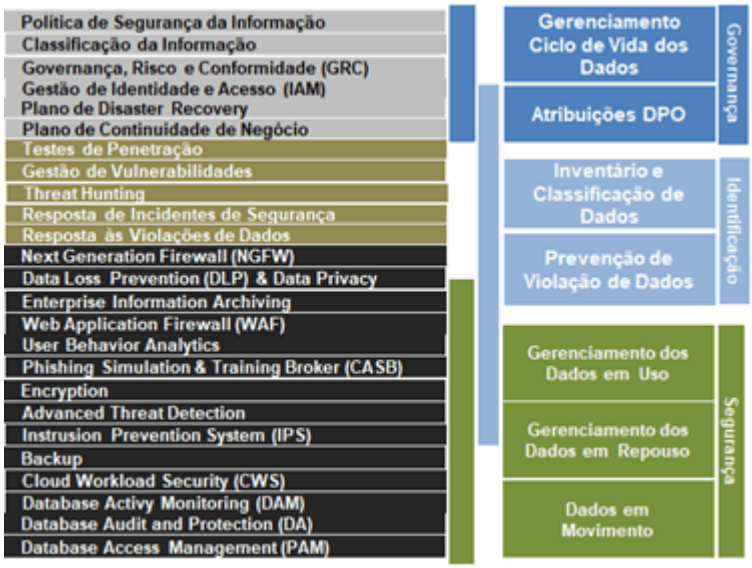
Etapa #7:Implementar controles de Segurança de Dados

Esta etapa é responsável por:

- implementar um conjunto de controles de Segurança da Informação voltados especificamente a Proteção dos Dados Pessoais mantidos nos sistemas de TI e bases de dados da empresa (manual e automatizado), considerando-se:
    - Passo 1: Incluir aspectos de Privacidade de Dados na Política de Segurança corporativa;
    - Passo 2: Incluir Privacidade de Dados na Política de Segurança da Informação;
    - Passo 3: Incluir Privacidade de Dados na Política de uso de recursos corporativos, aceitável;
    - Passo 4: Incluir Privacidade de Dados em Avaliações de Riscos de Segurança;
    - Passo 5: Implementar controles técnicos de Segurança de TI;
    - Passo 6: Implementar controles de segurança de recursos humanos;
    - Passo 7: Incluir Privacidade de Dados no planejamento de Continuidade de Negócios;
    - Passo 8: Desenvolver e implementar uma estratégia de prevenção de perda de dados;
    - Passo 9: Realizar testes regulares de segurança de dados;
    - Passo 10: Manter a certificação de segurança.

- **Resultado previsto:** Medidas e controles de Segurança de Dados implementados.





Resultados – Fase-3: Definição e Implementação

Dentre as 7 (sete) etapas acima consideradas, os seguintes **resultados são previstos:**

1. **Sistema de Classificação de Dados Pessoais – Etapa #1.**
2. **Procedimento para aprovação do processamento de dados pessoais – Etapa #2.**
3. **Documento de registro de Bases de Dados contendo Dados Pessoais – Etapa #3.**
4. **Desenvolver e implementar um sistema transferência internacional de dados pessoais – Etapa #4.**
5. **Atividades estratégicas, táticas e operacionais do dia-a-dia corporativo devida integrados com Dados Pessoais e Privacidade – Etapa #5.**
6. **Executar plano de treinamento corporativo para Dados Pessoais e Privacidade – Etapa #6.**
7. **Implementar controles de Segurança de Dados – Etapa #7.**

Resultado final: Desenvolver e implementar um conjunto de medidas de monitoração e controle de Proteção de Dados e Privacidade para a governança de Dados Pessoais de forma eficiente e eficaz.