LGPD | FASE-1: PREPARAÇÃO | JORNADA DE ADEQUAÇÃO | SGPD | SISTEMA DE GESTÃO DE PROTEÇÃO DE DADOS

PUBLICADO EM 28/12/2019 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-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 o mapeamento e consolidação de todos os processos corporativos envolvidos direta ou indiretamente com o processamento automatizado ou manual de dados pessoais, e de todas as necessidades, requisitos técnicos e operacionais da Proteção de Dados e a Privacidade que afetam a empresa, a organização.

A partir do mapeamento e consolidação dos processos corporativo, caracteriza-se a premissa básica para a identificação das leis, padrões e normas regulatórias relevantes relacionados à proteção de dados e privacidade, as quais o negócio corporativo está sujeito:

- Regulamentações setoriais: BACEN, CVM, ANVISA, etc.;
- Código de Defesa do Consumidor;
- Lei de Crimes Cibernéticos;
- Lei do Cadastro Positivo;
- Lei de Acesso à Informação;
- Marco Civil da Internet;
- Lei de Liberdade Econômica;
- Lei da Desburocratização;
- PCI, HIPPA, Governança, etc.;
- Outras Legislações e Regulamentações;
- GDPR – AEE (Área Econômica Europeia)- Lei Europeia de Proteção de Dados e Privacidade
- LGPD – Brasil – Lei Geral de Proteção de Dados

Como resultado final esperado desta Fase materializa-se um plano de ação em função dos requisitos técnicos e operacionais, dos processos consolidados, da legislação e normas regulatórias aos quais o negócio está sujeito, para preparar a empresa a gerenciar seus dados pessoais considerando-se a Proteção de Dados e Privacidade (PD&P).

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

Etapa #1: Realizar a Análise de Privacidade

Esta etapa é responsável por:

- consolidar uma visão corporativa do negócio quanto aos processos que se utilizam direta ou indiretamente Dados Pessoais;
- identificar todos os aspectos Legais e de Regulamentação aos quais o negócio está sujeito;
- avaliar o contexto corporativo quanto a prontidão requerida para Proteção e Privacidade de Dados;
- Gerar um Relatório consolidado respondendo aos seguintes questionamentos:
    - Quem envia Dados Pessoais e Dados Pessoais Sensíveis para a empresa?
    - Como a empresa recebe estes Dados Pessoais?
    - Qual o tipo de Dados Pessoais é coletado em cada ponto de entrada dos processos de Negócio?
    - Onde e como os Dados Pessoais são armazenados e mantidos?
    - Qual a política de acesso aos Dados Pessoais?
- **Resultado previsto:** Relatório de Análises de Proteção de Dados e Privacidade

Etapa #2: Coletar Leis de Privacidade

Esta etapa é responsável por:

- consolidar as legislações, regulamentações, regras, normas de proteção de dados e privacidade em nível nacional e internacional. identificar as leis, padrões e normas regulatórias relevantes relacionados à proteção de dados e privacidade, as quais o negócio corporativo está sujeito:
    - Regulamentações setoriais: BACEN, CVM, ANVISA, etc
    - Código de Defesa do Consumidor
    - Lei de Crimes Cibernéticos
    - Lei do Cadastro Positivo
    - Lei de Acesso à Informação
    - Marco Civil da Internet
    - Lei de Liberdade Econômica
    - Lei da Desburocratização
    - PCI, HIPPA, Governança, etc.
    - Outras Legislações e Regulamentações

        - GDPR – AEE – Lei Europeia de Proteção de Dados e Privacidade
        - LGPD – Brasil – Lei Geral de Proteção de Dados
    - alguns **Princípios de Legislação de Geral de Proteção de Dados** se fazem necessário um foco específico de mapeamento e consolidação:
        - Processamento legítimo
        - Finalidades específicas
        - Dados pessoais relevantes.
        - Dados pessoais precisam estar corretos e atualizados.
        - Dados pessoais devem ser processados somente durante o período necessário para o propósito previamente declarado.
    - **Resultado previsto:** Coletar Leis de Privacidade

Etapa #3: Analisar o impacto da Privacidade no negócio

Esta etapa é responsável por:

- revisar, estudar e entender os impactos dessas regras, regulamentos e padrões de proteção de dados e privacidade no dia-a-dia das operações corporativas.
- gerar um log de acompanhamento – Manual de Leis de Privacidade.
- **Resultado previsto:** Analisar o impacto da Privacidade no negócio

Etapa #4: Realizar Auditorias e Avaliações dos dados iniciais

Esta etapa é responsável por:

- executar uma Avaliação Inicial de Proteção de Dados corporativo, para identificar e divulgar como a empresa está lidando como as regulamentações e possíveis riscos existentes para o negócio de para os indivíduos.
- normas e guias de reguladores de mercado ou outras entidades – apoio.
- **Resultado previsto:** Realizar Auditorias e Avaliações dos dados iniciais

Etapa #5: Estabelecer a estrutura organizacional de Governança de Dados

Esta etapa é responsável por:

- criar Comitê de Governança de Dados
    - Revisar impactos e riscos
    - Assegurar que medidas de controles sejam implementadas para mitigação de riscos
- apontar e treinar os Papéis de Governança de Dados
    - Pelas melhores práticas o DPO | Encarregado de Proteção de Dados será identificado somente na Fase 2 e Etapa #2.
    - Identificar o Gerente de Seguranla da informação

        - Identificar todos os demais papéis envolvidos na qualidade de Dados Pessoais.
    - **Resultado previsto:** Estabelecer a estrutura organizacional de Governança de Dados.

Etapa #6: Estabelecer Fluxo de Dados e Inventário de Dados Pessoais

Esta etapa é responsável por:

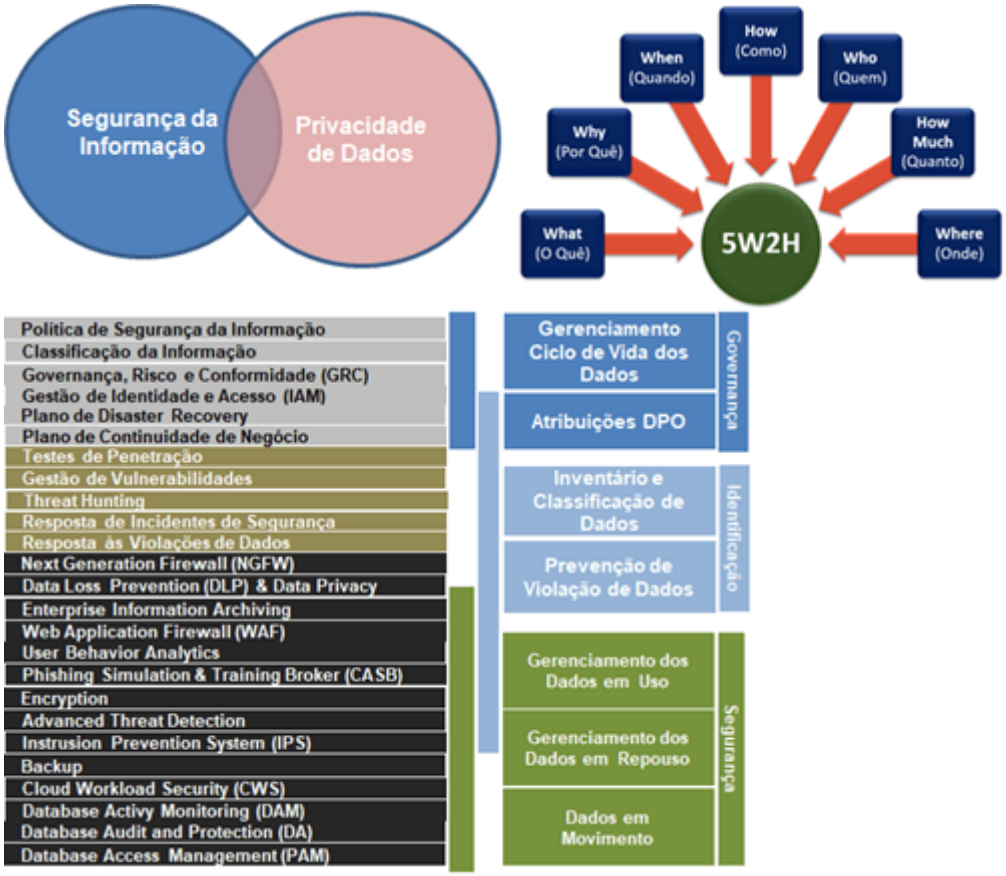
- criar e formalizar o Mapeamento e Inventário de Dados Pessoais mantidos por vários departamentos, sistemas, parceiros e terceiros, incluindo:
    - todos os formatos de Dados Pessoais: eletrônico e em papel;
    - identificação dos colaboradores responsáveis para cada um destes Dados Pessoais;
    - classificação do tipo de Dado Pessoal tratado: colaboradores, clientes, copropriedade com outras empresas, etc.
    - onde e como estes Dados Pessoais são mantidos e armazenados: servidores, dispositivos móveis, na nuvem, mídias, etc.
- **Resultado previsto:** Sistema de Fluxo de Dados, Inventário de Dados Pessoais e Política de Proteção de Dados.

Etapa #7: Estabelecer programa de Proteção de Dados e Privacidade

Esta etapa é responsável por:

- **Plano de Treinamento de Privacidade de Dados**:
  - Plano de comunicação;
  - Plano de conhecimento específico.
- **Estratégia Corporativa de Proteção de Dados e Privacidade – PD&P**
  - Cultura corporativa em Proteção de Dados e Privacidade
  - Escopo do programa corporativo de PD&P
  - Estabelece a matriz de responsabilidade do Encarregado da Proteção de Dados
  - Detalha a estratégia para alcançar as principais prioridades de PD&P

- **Programa de Proteção de Dados e Privacidade – PD&P**
    - Enfatiza o valor reconhecido pela organização quanto a Proteção de Dados e Privacidade
    - Identifica os principais objetivos do Programa Corporativo de PD&P
    - Detalha a estratégia de PD&P e os Controles de Governança para se atingir os objetivos de Privacidade previamente definidos.
- **Resultado previsto:** Execução do Plano de Treinamento em Privacidade e do Programa de Proteção de Dados & Privacidade.



Etapa #8: Esboçar Planos de Implementação de ações de Proteção de Dados e Privacidade

Esta etapa é responsável por:

- consolidar um Relatório para o Board Corporativo embasado nos resultados das Etapas #1 a #7:
    - consolidação das informações das etapas de análise preparação
    - orçamento para implementação
    - conjunto de Planos de Ações específicos para a execução do processo completo de Proteção de Dados e Privacidade de cada Fase.
- **Resultado previsto:** Orçamento da estruturação da Gestão de Proteção de Dados e Planos de Implementação de Ações de Proteção de Dados e Privacidade.

Resultados – Fase-1: Preparação

Dentre as 8 (oito) etapas acima consideradas, os seguintes **resultados são 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