LGPD | FASE-2: ORGANIZAÇÃO | JORNADA DE ADEQUAÇÃO | SGPD | SISTEMA DE GESTÃO DE PROTEÇÃO DE DADOS

PUBLICADO EM 29/12/2019 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-2: Organização

O principal objetivo desta fase considerada dentro do sistema proposto, é 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;
- envolver e comprometer todas as partes envolvidas com 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:** Atribuir 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 Sênior – 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.
- **Etapa #5:** Estabelecer e manter um plano de comunicação corporativa contínuo 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.

Etapa #1: Definir e implementar o “como manter” o programa, as políticas e controles de governança de privacidade de dados.

Esta etapa é responsável por:

- dar sustentação a estratégia e ao programa de Proteção de Dados e Privacidade definidos na Fase-1 de Preparação.
- definir e implementar um conjunto de processos e procedimentos que garantam a Política de Privacidade (adequação às sustentações e mudanças contínuas nos requisitos legais, regulamentadores e contratuais) através de direcionamentos e controles corporativos de Governança de Dados com orientações específicas para a cultura organizacional quanto a coleta, uso, processamento e proteção, com o objetivo de se mitigar os riscos de violação de dados pessoais.
- atuar junto ao Board Estratégico para que o programa de Proteção e Privacidade de Dados (PD&P) esteja apoiado na declaração da missão da empresa considerando-se o valor que a organização atribui e os principais objetivos relacionados à proteção e privacidade de dados, assim como as estratégias e controles de governança para se alcançar os objetivos de privacidade.
- **Resultado previsto:** Consolidar a Estratégia de Proteção de Dados e Privacidade atualizada, o Programa de Proteção de Dados e Privacidade atualizado e os Controles de Governança de Dados atualizados.

Etapa #2: Atribuir e manter a matriz de atribuições e responsabilidades pela Proteção de Dados e Privacidade – Matriz RACI.

Esta etapa é responsável por:

- definir as atribuições e responsabilidades pelos aspectos operacionais do programa de Proteção de Dados e Privacidade a um indivíduo, considerando-se colaboradores dos departamentos jurídico, de conformidade, de TI, de segurança ou de outros departamentos de gerenciamento.
- **Resultado previsto:** Consolidar as atribuições e responsabilidades do Encarregado da Proteção de Dados e Privacidade e anunciar a nomeação do Encarregado da Proteção de Dados e Privacidade

Etapa #3: Definir e implementar o “como manter” o envolvimento dos níveis táticos e estratégicos da organização – Gerência Sênior – na Proteção de Dados e Privacidade.

Esta etapa é responsável por:

- definir e implementar o “modus operandus” para o contínuo envolvimento do nível tático e estratégico das empresas e organizações para se obter melhores resultados dos direcionamentos definidos para a Proteção e Privacidade de dados, considerando-se:
    - contínua comunicação da relevância da Proteção de Dados e Privacidade à equipe de gerência diretamente subordinada;
    - participação ativa e posicionamento contínuo de todas as iniciativas de Proteção de Dados e Privacidade, e;
    - garantir os aspectos financeiros adequados para apoiar a função de Proteção de Dados e Privacidade.
- **Resultado previsto:** Plano de Comunicação para todas questões de Proteção de Dados e Privacidade – versão-1

Etapa #4: Estabelecer e manter a continuidade do compromisso de todos os níveis hierárquicos da organização com a Proteção de Dados e Privacidade

Esta etapa é responsável por:

- estruturar uma rede / estrutura corporativa de Proteção de Dados e Privacidade, desempenhando funções específicas e obtendo o comprometimento das equipes;
    - os membros desta Rede podem trabalhar em diferentes grupos funcionais ou departamentos para facilitar o entendimento dos riscos de Proteção de Dados e Privacidade aplicáveis a esse grupo ou departamento funcional de negócios (similar a um membro da CIPA);
    - os responsáveis pela Proteção de Dados e Privacidade têm funções e responsabilidades claras, definidas nas descrições de cargo e outros documentos relacionados a trabalho, como Contrato de Trabalho, Código de Conduta, etc.
    - dentre as funções a serem desempenhadas temos: Encarregado da Proteção de Dados (DPO), Gerentes de Privacidade; Analistas de Privacidade; Comitê de Proteção de Dados e Privacidade, Equipe de Resposta a Incidentes de Violação de Dados, etc.
- **Resultado previsto:** Formalização e aceite formal na concordância e adesão à Política de Proteção de Dados e à Política de Privacidade de cada membro da equipe quanto às suas ações com relação ao tratamento de dados pessoais, Plano de Comunicação para todas questões de Proteção de Dados e Privacidade-v2, Estrutura corporativa de PD&P e Função de Proteção de Dados e Privacidade incluída nas descrições de cargos, Código de Conduta, Manual do Funcionário e Cópia individual da Política de Proteção de Dados e Privacidade

Etapa #5: Estabelecer e manter um plano de comunicação corporativa regular para

direcionamentos, questões e problemas de Proteção de Dados e Privacidade.

Esta etapa é responsável por:

- Identificar os colaboradores responsáveis pela manutenção no dia-a-dia da Proteção de Dados e Privacidade devem se comunicar regularmente entre si para:
    - Aprendizagem e disseminação contínua sobre o uso de dados pessoais em todas as funções e no pensamento do dia-a-dia da empresa;
    - Auxiliar proativamente na construção de Proteção de Dados e Privacidade em todos os sistemas, serviços, produtos e projetos em andamento;
    - Tratar as diferentes perspectivas sobre Proteção de Dados e Privacidade de dados, e;
    - Permitir, facilitar e apoiar os colaboradores a atingir seus objetivos e metas enquanto Proteção de Dados e Privacidade.
- **Resultado previsto:** Plano de Comunicação para todas questões de PD&P-v3 e Plano atualizado de conscientização, comunicação e treinamento relacionado ao Programa de Proteção de Dados e Privacidade.

Etapa #6: Manter o engajamento das partes interessadas em Proteção de Dados e Privacidade

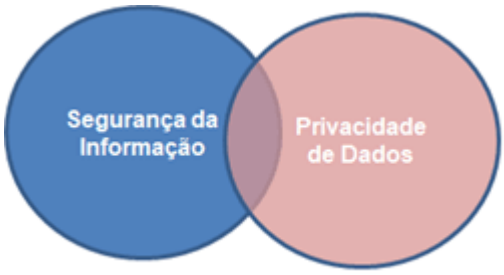
Esta etapa é responsável por:

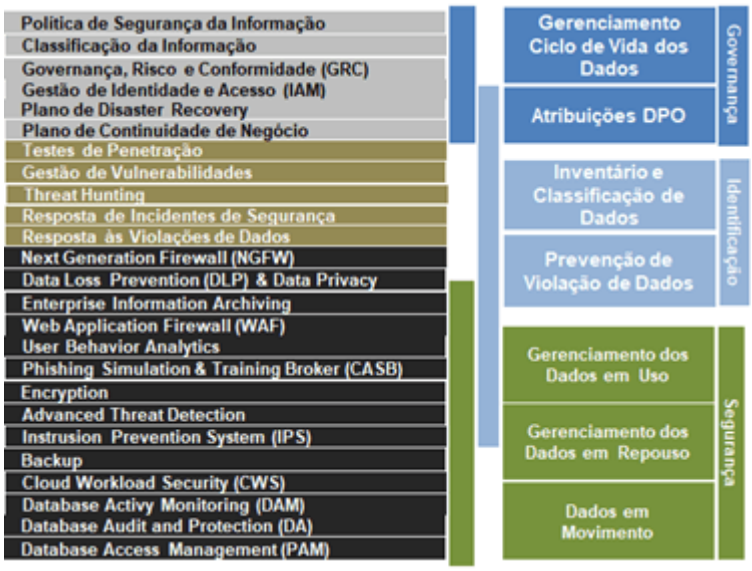
- abordar proativa e continuamente os aspectos corporativos relacionados à Privacidade e Proteção de Dados, bem como responder efetivamente aos problemas de relevantes e os respectivos impactos às partes interessadas em toda a empresa, inerentes à Função de Proteção de Dados e Privacidade:
    - Realiza comunicações informais ou ad hoc com indivíduos cujas responsabilidades podem não incluir proteção de dados e privacidade;
    - Participação ativa em comitês corporativos ou unidades de negócios cujas atividades podem impactar a proteção de dados e na privacidade (por exemplo, segurança da informação, marketing, etc.);
    - Comunicação periódica e contínua sobre questões de proteção de dados e privacidade com parceiros externos (provedores de nuvem, provedores de serviços de informação, fornecedores de manutenção de aplicativos etc.) diretamente envolvidos no processamento de dados pessoais.
- **Resultado previsto:** Plano de Comunicação para todas questões de Proteção de Dados e Privacidade-vFinal.

Etapa #7: Implementar e operar sistemas informatizados para a sustentação da Proteção de Dados e Privacidade corporativa.

Esta etapa é responsável por:

- As soluções de proteção de dados devem adotar uma abordagem abrangente, de ponta a ponta, que começa identificando dados de risco e desenvolvendo uma estratégia contínua de proteção de dados que responda a todas as ameaças em potencial – antes que as ameaças sejam identificadas:
    - verificação dos arquivos originais e de backup através de algoritmos de hash;
    - criptografar dados em trânsito e em repouso;
    - fornecer uma interface centralizada de conformidade de gerenciamento de dados;
    - relatórios de sucessos e falhas de backup;
    - gerenciar todos os aspectos do processo de regras corporativas vinculativas (BCR);
    - medição e relatórios sobre o cumprimento das leis nacionais, etc;
- **Resultado previsto:** Sistema informatizado de Proteção de Dados e Privacidade.





Resultados – Fase-2: Organização

Dentre as 7 (sete) etapas acima consideradas, os seguintes **resultados são 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: Uma organização preparada para ser eficiente no tratamento e gerenciamento dos riscos envolvidos na Proteção de Dados e Privacidade