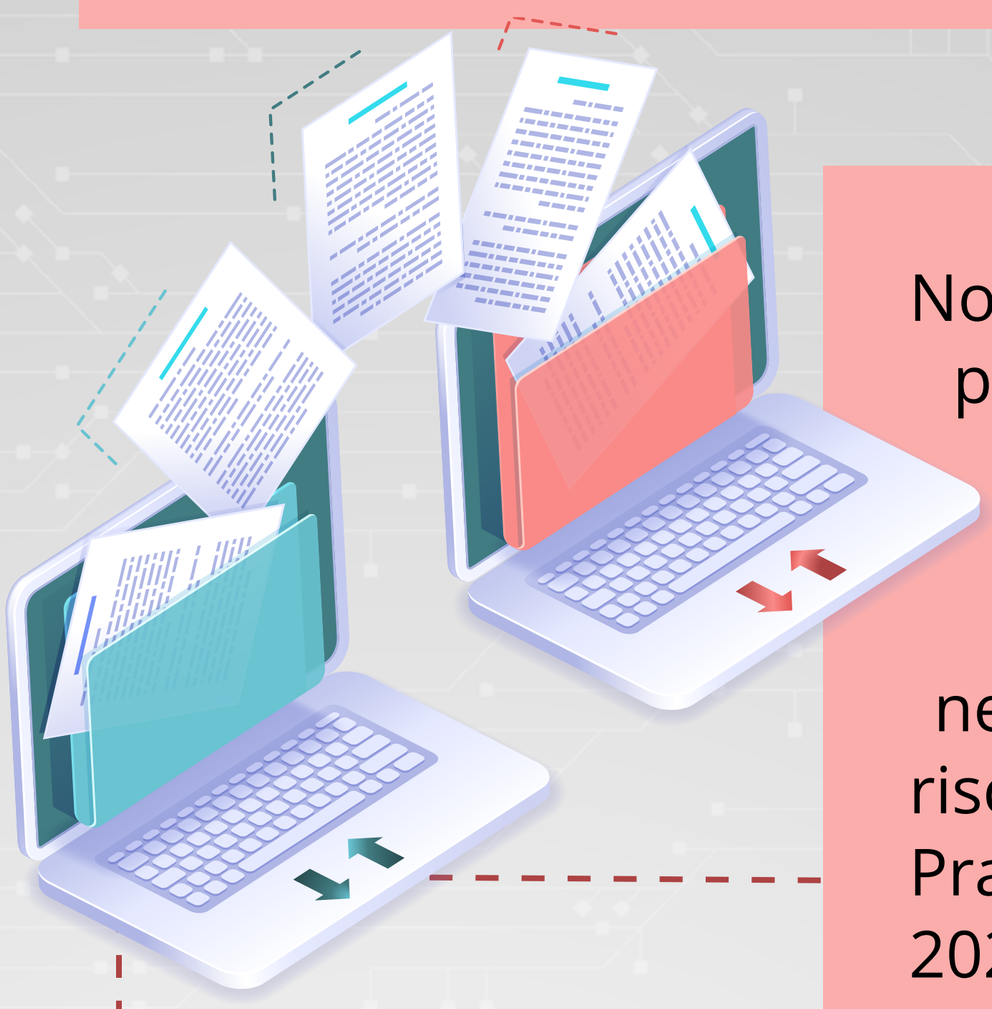
MEDINDO O PROGRAMA DE PRIVACIDADE

Edição 1.0 – Novembro/2022

PRADO VIDIGAL

Privacidade & Digital

O futuro da área de privacidade nas organizações passa pela constante evolução e consolidação da maturidade de programas de privacidade. Uma vez terminados projetos específicos que tinham como objetivo estruturar e revisar processos e políticas minimamente necessários para se atender aos novos requisitos legais, empresas comprometidas com o tema agora enfrentam a missão de definir seus níveis de maturidade em cada uma das frentes que compõem um programa de privacidade e, com isso, viabilizar a compreensão dos pontos fortes e fracos. Em outras palavras, é momento de medir a efetividade daquilo que foi (ou está sendo) estruturado e trazer objetividade para o programa de privacidade, definindo metas de melhoria e níveis de tolerância. Sem um “painel de controle” composto pelas metas e métricas definidas pela organização, a gestão da privacidade fica prejudicada por não se ter indicadores nem clareza em relação às prioridades e próximas ações a serem adotadas.



No entanto, criar métricas para o programa de privacidade não é tarefa trivial, pois depende de ações estratégicas que levem em consideração as particularidades de cada organização, especialmente modelo de negócio, valores, recursos, cultura e apetite a riscos. Pensando em amenizar esse desafio, o Prado Vidigal Advogados realizou em outubro de 2022 evento com a presença de representantes de variadas empresas com o objetivo de, de forma colaborativa, reunir métricas exemplificativas que, com as devidas adaptações e ponderações, podem ser úteis a programas de privacidade de variadas organizações. Além dos estudos e contribuições do próprio escritório, o processo de idealização de tais métricas contou com a participação de representantes de 34 empresas que são referências nos seguintes setores: tecnologia, telecomunicações, financeiro, seguros, saúde, farmacêutico, indústria, energia, ensino e pesquisa.

O resultado deste trabalho feito pelo escritório em parceria com seus clientes, parceiros e apoiadores é apresentado neste documento, que pretende ser útil a equipes de privacidade de organizações que atualmente enfrentam os seguintes desafios e dilemas:

Como apresentar resultados objetivos do programa de privacidade para a alta gestão da organização e eventuais outros stakeholders?

O que mais fazer quando a sensação é de que muito já foi feito?

Onde investir e o que priorizar para os próximos 12 meses?

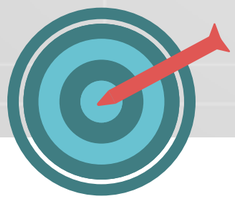
Como avaliar se os processos de privacidade que foram estruturados estão realmente funcionando como deveriam?

METAS X MÉTRICAS

Embora andem de mãos dadas, os conceitos de “metas” e “métricas” não se confundem. De maneira bastante resumida, com o objetivo de padronizarmos entendimentos para fins de interpretação deste documento, vamos considerar que:

- *Metas:* são os objetivos esperados para determinado eixo do programa de privacidade;

- *Métricas:* são medidas quantificáveis que servem para se apurar o resultado de uma ação ou de um processo.



Para a criação das metas, uma boa dica é seguir a metodologia SMART, amplamente difundida no contexto corporativo.

SPECIFIC *(específica)*

metas devem ser específicas para que seu objetivo seja claro e entendido por todos os envolvidos.

MEASURABLE *(mensurável)*

é preciso ser capaz de se estipular métricas e indicadores para que se acompanhe o atingimento (ou não) das metas estipuladas.

ATTAINABLE *(atingível)*

embora devam apresentar certo nível de desafio, metas irreais e impossíveis de serem alcançadas são desmotivadoras e inúteis ao progresso buscado.

RELEVANT *(relevante)*

metas devem ser sempre úteis e importantes para se atingir um objetivo maior, sendo instrumentos de meio (e não fim).

TIME BASED *(temporal)*

metas devem sempre estar vinculadas a um prazo determinado.

Exemplo:

PILAR	Conscientização
META	Ter 100% dos colaboradores treinados até dezembro/2023
POSSÍVEIS MÉTRICAS	nº de áreas treinadas
	% de colaboradores presentes em treinamentos
	% de acerto de respostas em quiz realizado após o treinamento

POSSÍVEIS MÉTRICAS PARA PROGRAMAS DE PRIVACIDADE

O exercício de construção de métricas para o programa de privacidade capitaneado pelo escritório teve como ponto de partida 5 (cinco) pilares bastante comuns em programas de privacidade:

1. ***inventário e mapeamento***
2. ***conscientização***
3. ***gestão de riscos***
4. ***incidentes***
5. ***direitos dos titulares***

Diante disso, a partir de casos simulados, representantes das empresas participantes desenharam metas e, consequentemente, métricas na intenção de mensurar os principais objetivos do programa de privacidade.

Abaixo apresentamos o resultado das métricas (não quantificadas) que, no entendimento do escritório, podem ser úteis aos programas de privacidade de variadas organizações. Vale destacar que a lista é exemplificativa, sendo que a aderência das métricas à realidade de cada organização dependerá dos objetivos e demais particularidades do respectivo programa de privacidade.

Inventário e Mapeamento

- ✓ *nº total e/ou % de sistemas mapeados*
- ✓ *nº total e/ou % de áreas mapeadas*
- ✓ *nº total e/ou % de áreas críticas mapeadas*
- ✓ *nº total e/ou % de unidades de negócio mapeadas*
- ✓ *nº total e/ou % de fornecedores identificados*
- ✓ *nº total e/ou % de produtos/soluções mapeados*
- ✓ *nº total de colaboradores entrevistados*
- ✓ *nº total de processos mapeados*
- ✓ *tempo decorrido entre o surgimento de um novo processo e seu registro no inventário/registro de operações de tratamento*
- ✓ *tempo decorrido entre as atualizações do inventário/ mapeamento*
- ✓ *tempo despendido para conclusão de processos de atualização do inventário/registro de operações de tratamento*

Conscientização

- ✓ *nº total de treinamentos realizados*
- ✓ *nº total e/ou % de treinamentos realizados por tema*
- ✓ *nº total de treinamentos realizados por área*
- ✓ *nº total e/ou % de áreas treinadas*
- ✓ *nº total e/ou % de treinamentos realizados por público-alvo*
- ✓ *nº total e/ou % de colaboradores treinados*
- ✓ *nº total e/ou % de colaboradores treinados de acordo com cargo/ posição*
- ✓ *nº total e/ou % de colaboradores de áreas críticas treinados*
- ✓ *nº total e/ou % de colaboradores presentes em treinamentos*
- ✓ *nº total e/ou % de fornecedores/terceiros treinados*
- ✓ *nº total e/ou % de colaboradores treinados durante o onboarding*
- ✓ *tempo médio para conclusão do treinamento de novos colaboradores a contar do ingresso na organização*
- ✓ *nº total e/ou % de colaboradores com desempenho satisfatório em quiz sobre o tema*
- ✓ *nº total e/ou % de colaboradores certificados em privacidade*
- ✓ *nº total de materiais de conscientização criados/disseminados*
- ✓ *nº total e/ou % de acessos/leitura de materiais de conscientização*
- ✓ *nº total de dúvidas/questionamentos direcionados ao time de privacidade*

Gestão de Riscos

- ✓ *nº total e/ou % de atividades/processos com risco avaliado*
- ✓ *nº total e/ou % de atividades/processos classificados como de risco alto*
- ✓ *nº total e/ou % de fornecedores/terceiros avaliados via questionário/ ferramenta*
- ✓ *nº total e/ou % de fornecedores/terceiros com score de risco satisfatório*
- ✓ *nº total e/ou % de fornecedores/terceiros de risco alto*
- ✓ *nº total e/ou % de fornecedores/terceiros que contam com cláusulas e/ ou acordos para tratamento de dados formalizados com a organização*
- ✓ *nº total e/ou % de medidas mitigatórias implementadas*
- ✓ *nº total de avaliações de impacto realizadas*
- ✓ *nº total de projetos e/ou novas atividades analisadas pelo time de privacidade*
- ✓ *nº total de projetos e/ou novas atividades de áreas críticas analisadas pelo time de privacidade*
- ✓ *nº total e/ou % de projetos e/ou novas atividades classificadas como de alto risco*
- ✓ *nº de projetos e/ou novas atividades analisadas de cada área*
- ✓ *tempo médio de resposta do time de privacidade para análise de projetos e/ou novas atividades*
- ✓ *tempo médio despendido para a implementação das medidas mitigatórias*
- ✓ *valores (R$) despendidos para a implementação das medidas mitigatórias*

Incidentes

- ✓ *nº total de incidentes identificados*
- ✓ *nº total e/ou % de incidentes por tipo/criticidade/unidade de negócio/entidade/região*
- ✓ *nº total e/ou % de incidentes de origem externa e interna*
- ✓ *nº total de titulares afetados*
- ✓ *tempo médio para identificação de incidentes*
- ✓ *tempo médio para investigação de incidentes*
- ✓ *tempo médio para conclusão de respostas a incidentes*
- ✓ *tempo médio para conclusão da implementação de medidas corretivas*
- ✓ *% de respostas a incidentes concluídas dentro do prazo esperado*
- ✓ *nº total de demandas de titulares após a comunicação de incidentes*
- ✓ *nº total de investigações iniciadas por autoridades competentes após a comunicação de incidentes*
- ✓ *valores (R$) despendidos para contenção de incidentes*
- ✓ *valores (R$) despendidos para contratação de prestadores de serviço durante a contenção de incidentes*
- ✓ *% de incidentes em que a causa raiz foi identificada*
- ✓ *% de incidentes cujas ações corretivas foram adotadas adequadamente*
- ✓ *nº total e/ou % de incidentes notificados a reguladores e titulares de dados*
- ✓ *nº total de exercícios de simulação de incidentes realizados*
- ✓ *% de alertas/suspeitas que resultam em falso positivo*

Direitos dos Titulares

- ✓ *nº total de solicitações recebidas*
- ✓ *nº total de solicitações em processamento*
- ✓ *nº total de solicitações concluídas*
- ✓ *nº total e/ou % de solicitações concluídas dentro do prazo estipulado*
- ✓ *tempo médio de resposta*
- ✓ *tempo médio para validação de identidade do titular*
- ✓ *nº e/ou % de solicitações negadas*
- ✓ *% de satisfação dos titulares em relação às respostas recebidas*
- ✓ *nº e/ou % de solicitações recebidas por tipo de direito*
- ✓ *nº e/ou % de reclamações de titulares à ANPD*

*FRAMEWORKS SÃO **TENDÊNCIA** PARA OS PROGRAMAS DE PRIVACIDADE*

Medir adequadamente o programa de privacidade e estabelecer metas de melhoria é, atualmente, uma das principais tarefas de times de privacidade de empresas que já passaram por aquilo que se convencionou chamar de “projeto de adequação” à Lei Geral de Proteção de Dados (LGPD).

Nesse sentido, em empresas que pretendem reforçar continuamente suas práticas de privacidade, uma das principais atividades tem sido a edificação de framework de privacidade próprio da organização, a partir de influências externas (como o NIST Privacy Framework e a própria LGPD).

As vantagens de se construir um framework próprio da organização, aderente às suas particularidades, são inúmeras, sendo que, ao final de sua estruturação, o time de privacidade passa a contar com ferramenta que reúne metas e métricas para a gestão eficiente do tema, trazendo indicativos do que existe em termos de governança de privacidade, o que pode ser melhorado e o que é prioritário.

*RECURSOS **ÚTEIS***

Abaixo, elencamos alguns materiais que embasaram a elaboração do presente documento e que podem ser úteis às organizações na missão de construir suas próprias metas e métricas de privacidade:

- LGPD Crosswalk by Prado Vidigal Advogados
- Sua organização não deve mais fazer um “projeto de adequação à LGPD”
- Measuring privacy programs: The role of metrics
- Future of Privacy Forum: Privacy Metrics Report

SOBRE O PRADO VIDIGAL

Somos escritório de advocacia boutique especializado em Direito e Tecnologia, sendo um dos top of mind em privacidade e proteção de dados no Brasil segundo rankings e publicações nacionais e internacionais.

Fale conosco

pradovidigal.com.br

linkedin.com/company/pradovidigal/

@pradovidigal

PRADO VIDIGAL

Privacidade & Digital