9º CONGRESSO INTERNACIONAL DE COMPLIANCE

LGPD
A jornada de implementação de um programa de proteção de dados em 2022

TÍTULO DA APRESENTAÇÃO

Subtítulo da apresentação

LGPD
A jornada de implementação de um programa de proteção de dados em 2022

01 Implantação do Programa

02 Principais Desafios

03 Gestão de Risco

04 Monitoramento

GESTÃO DE RISCOS

Objetivo

A avaliação de riscos deve ser realizada periodicamente com o objetivo de identificar e avaliar os riscos.

Deverá ser atualizada quando mudanças significativas ocorrerem no negócio, como por exemplo:

- O negócio, atividade ou projeto apresentarem risco alto;
- Violações sejam suspeitas ou identificadas;
- Atualizações regulatórias;
- Não-conformidades identificadas em monitoramentos, auditorias internas e externas;
- Expansão para nova localização geográfica/mercado.

GESTÃO DE RISCOS

Probabilidade	Nota	Frequência	Critério
Quase certo (de 90% a 100%)	5	Mais de 1 vez por mês	Esperado ocorrer na maioria das vezes - mais de 60 vezes a cada 5 anos
Provável (de 70% a 90%)	4	Mais de 1 vez por semestre até 1 vez por mês	Provável que ocorra em grande parte das vezes - de 11 a 60 vezes a cada 5 anos
Possível (de 30% a 70%)	3	1 vez por ano a uma vez por semestre	Pode ocorrer em algum momento - de 5 a 10 vezes a cada 5 anos
Baixa (de 10% a 30%)	2	Menos de uma vez por ano	Poderia ocorrer em circunstâncias excepcionais - de 3 ou 4 vezes a cada 5 anos
Raro% (até 10%)	1	Menos de uma vez em 5 anos	Poderia acontecer em circunstâncias raras - até 1 vez a cada 5 anos

GESTÃO DE RISCOS

Impacto	Nota	Critério
Alto	**5**	**Impacto para o Titular do Dado** ● Consequências irreversíveis tais como fraude ou incapacidade de trabalhar, danos físicos, morais - ou psicológicos a longo prazo, morte etc. **Impacto para a Empresa** ● Exposição negativa a nível nacional e/ou internacional. ● Eventos/processos relacionados ao descumprimento de regulamentação e/ou de legislação, movidos contra a empresa resultando em grades penalizações e/ou multas e/ou impedimento de operações. **Registros** ● Dados Pessoais de Clientes ou Público em Geral – maior ou igual a 10.000 registros ● Dados Pessoais de Funcionários – maior ou igual a 70% dos registros ● Dados Pessoais de Terceiros – maior ou igual a 70% dos registros ● Dados Pessoais Sensíveis, crianças ou adolescentes, independente do volume

GESTÃO DE RISCOS

Impacto	Nota	Critério
Significativo	**3**	**Impacto para o Titular do Dado** • Consequências que podem ser superadas, embora com sérias dificuldades como lista negra de bancos ou proteção ao crédito, perda de emprego, intimação, piora da saúde etc. **Impacto para a Empresa** • Exposição negativa a nível estadual. Eventos/processos relacionados ao descumprimento de regulamentação e/ou de legislação, movidos contra a empresa resultando em penalizações e/ou multas e/ou restrições nas operações. **Registros** • Dados Pessoais de Clientes ou Público em Geral – menor ou igual a 10.000 registros • Dados Pessoais de Funcionários – maior ou igual a 70% dos registros • Dados Pessoais de Terceiros – maior ou igual a 70% dos registros

GESTÃO DE RISCOS

Impacto	Nota	Critério
Moderado	**3**	**Impacto para o Titular do Dado** ● Inconvenientes significativos, que eles serão capazes de superar, apesar de algumas dificuldades com custos extras, negação de acesso a serviços de negócios, falta de entendimento e estresse. **Impacto para a Empresa** ● Exposição negativa a nível municipal ● Notificações/advertências com necessidade de estabelecer provisão para penalizações e multas dos órgãos fiscalizadores/reguladores. **Volume** ● Dados Pessoais de Clientes ou Público em Geral – entre 1.001 e 9.999 registros ● Dados Pessoais de Funcionários e/ou Terceiros – entre 51% e 69% dos registros

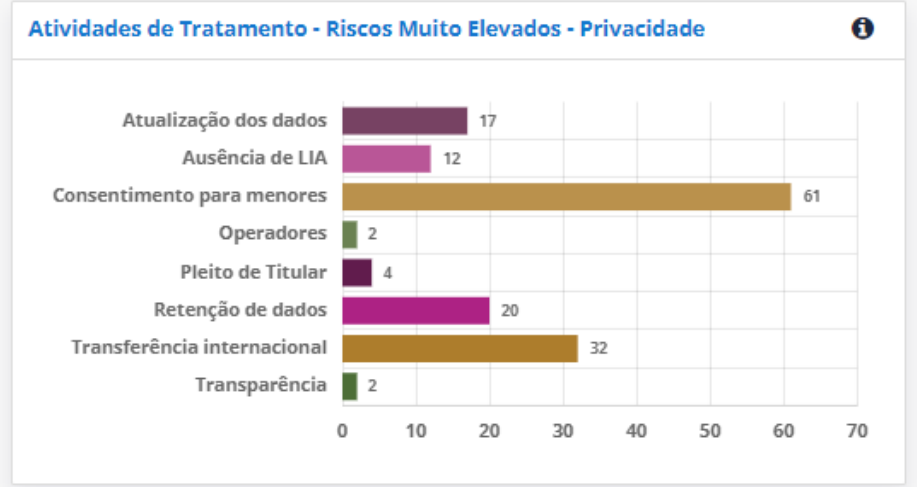
GESTÃO DE RISCOS

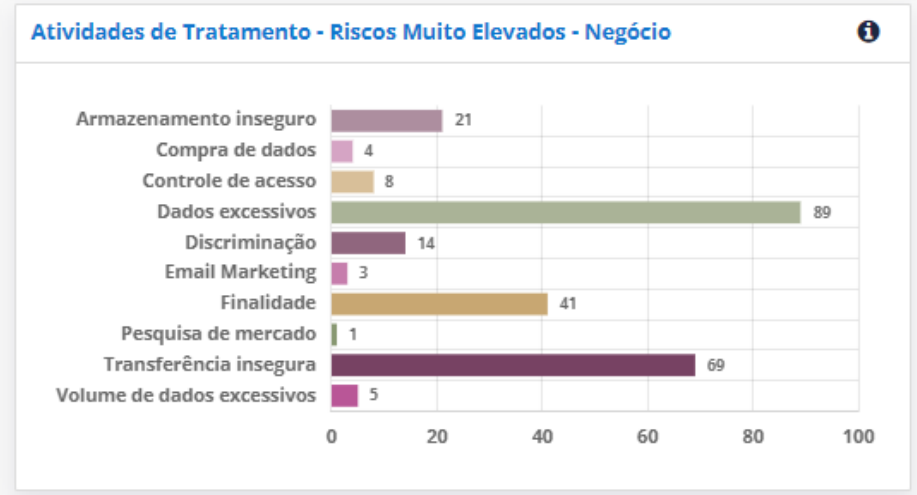
Impacto	Nota	Critério
Baixo	**2**	**Impacto para o Titular do Dado:** ● Os Titulares não serão afetados ou sofrerão inconvenientes que podem ser facilmente superados. **Impacto para a Empresa:** ● Sem penalizações e multas dos órgãos fiscalizadores/regulatórios. **Registro:** ● Dados Pessoais de Clientes ou Público em Geral – até 1.000 registros ● Dados Pessoais de Funcionários e Terceiros – até 50% dos registros ● O Dado Pessoal envolvido já é público.

GESTÃO DE RISCOS

Impacto	Nota	Critério
Mínimo	**1**	**Impacto para o Titular do Dado:** ● Não terão consequências em decorrência do vazamento. **Impacto para a Empresa:** ● Exposição negativa exclusiva junto ao público interno (empregados) ● Sem penalizações e multas dos órgãos fiscalizadores/ regulatórios. **Registro:** ● Dados Pessoais de Clientes – até 500 registros ● Dados Pessoais de Funcionários e Terceiros – até 10% dos registros ● O Dado Pessoal envolvido é público ou está anonimizado.

GESTÃO DE RISCOS





ID	Nome do risco	Modelo de risco	Descrição	Nível de risco residual	Pontuação
6622	Violação do Principio de Finalidade (...	R.BRK.01 - Finalidade	Tratamento de dados pessoais se...	Muito elevado	
6621	Violação do Princípio de Segurança e...	R.BRK.16 - Controle de Acesso - SAN	Ausência de segurança para coibir...	Muito elevado	
6591	Violação do Princípio de Segurança e...	R.BRK.39 - Extração de Dados Pess...	Ausência de validação da área de ...	Muito elevado	
6572	Violação do Princípio de Segurança e...	R.BRK.27 - Transferência insegura ...	Ausência de segurança para coibir...	Muito elevado	
6557	Violação do Principio de Necessidad...	R.BRK.10 - Volume de dados exces...	Uso de grande volume de dados p...	Muito elevado	
6553	Violação do Princípio de Segurança e...	R.BRK.28 - Armazenamento insegu...	Ausência de segurança para coibir...	Muito elevado	
6546	Violação do Principio de Finalidade (...	R.BRK.01 - Finalidade	Tratamento de dados pessoais se...	Muito elevado	
6539	Violação do Princípio de Necessidad...	R.BRK.08 - Dados Excessivos	Uso de dados pessoais excessivos ...	Elevado	
6533	Violação do Princípio de Necessidad...	R.BRK.08 - Dados Excessivos	Uso de dados pessoais excessivos ...	Muito elevado	
6491	Violação do Principio de Necessidad...	R.BRK.10 - Volume de dados exces...	Uso de grande volume de dados p...	Muito elevado	
6434	Violação do Princípio de Segurança e...	R.BRK.27 - Transferência insegura ...	Ausência de segurança para coibir...	Muito elevado	
6419	Violação do Princípio de Segurança e...	R.BRK.27 - Transferência insegura ...	Ausência de segurança para coibir...	Muito elevado	
6412	Violação do Princípio de Segurança e...	R.BRK.27 - Transferência insegura ...	Ausência de segurança para coibir...	Muito elevado	
6404	Violação do Princípio de Segurança e...	R.BRK.27 - Transferência insegura ...	Ausência de segurança para coibir...	Muito elevado	
6403	Violação do Princípio de Necessidad...	R.BRK.08 - Dados Excessivos	Uso de dados pessoais excessivos ...	Muito elevado	
6394	Violação do Princípio de Segurança e...	R.BRK.27 - Transferência insegura ...	Ausência de segurança para coibir...	Muito elevado	
6391	Violação do Princípio de Necessidad...	R.BRK.08 - Dados Excessivos	Uso de dados pessoais excessivos ...	Muito elevado	
6373	Violação do Princípio de Segurança e...	R.BRK.27 - Transferência insegura ...	Ausência de segurança para coibir...	Elevado	

MONITORAMENTO DO PROGRAMA

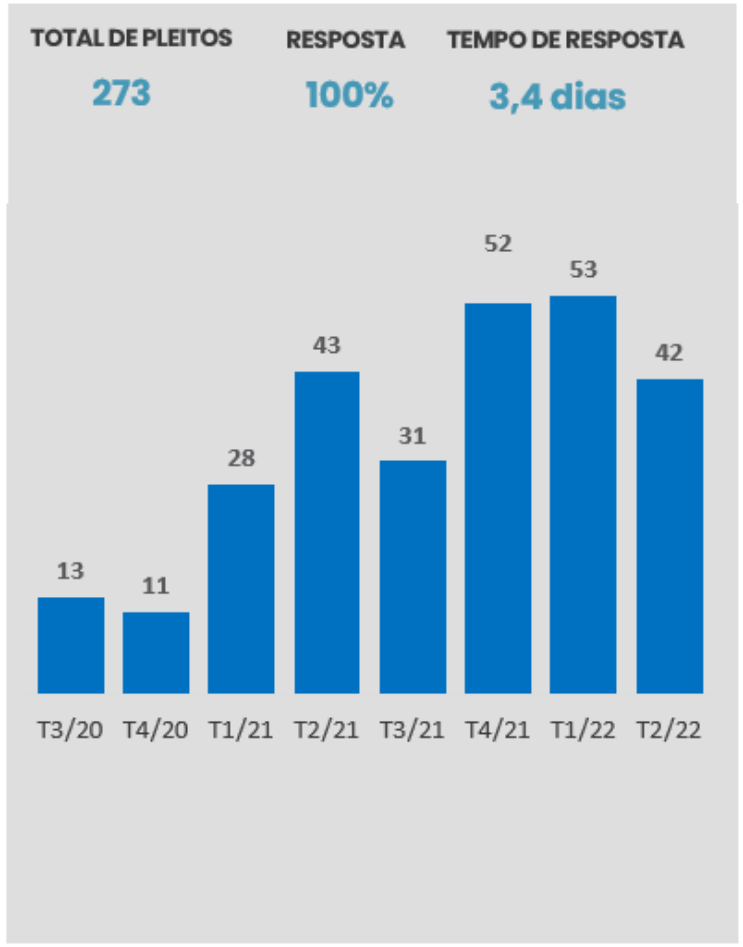
Objetivo

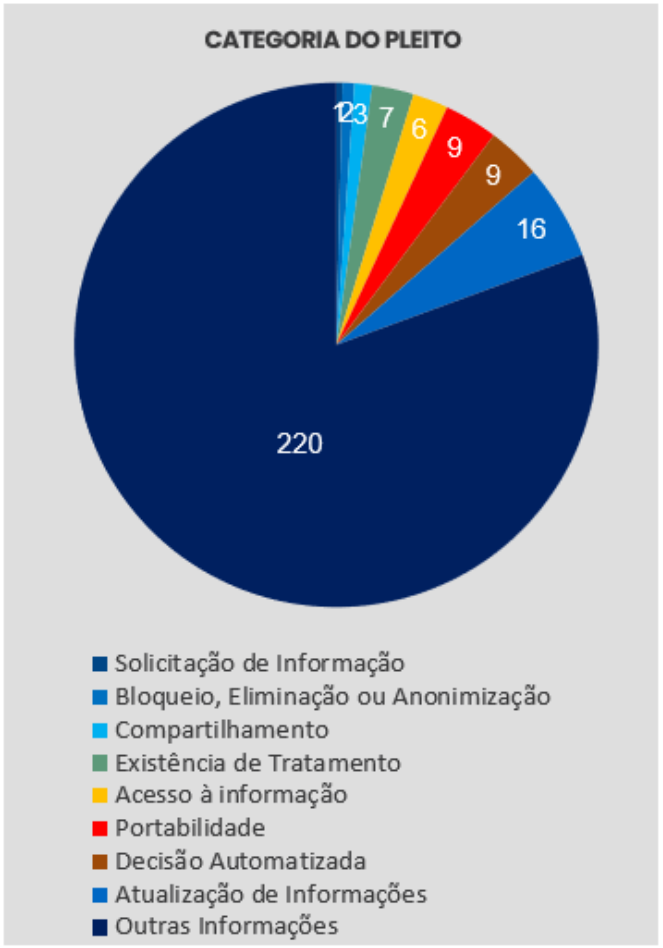
Verificar a efetiva implementação do programa a fim de identificar riscos e pontos falhos que possam ensejar correções e aprimoramentos. A análise do resultado do trabalho de monitoramento servirá para retroalimentar a matriz de riscos.

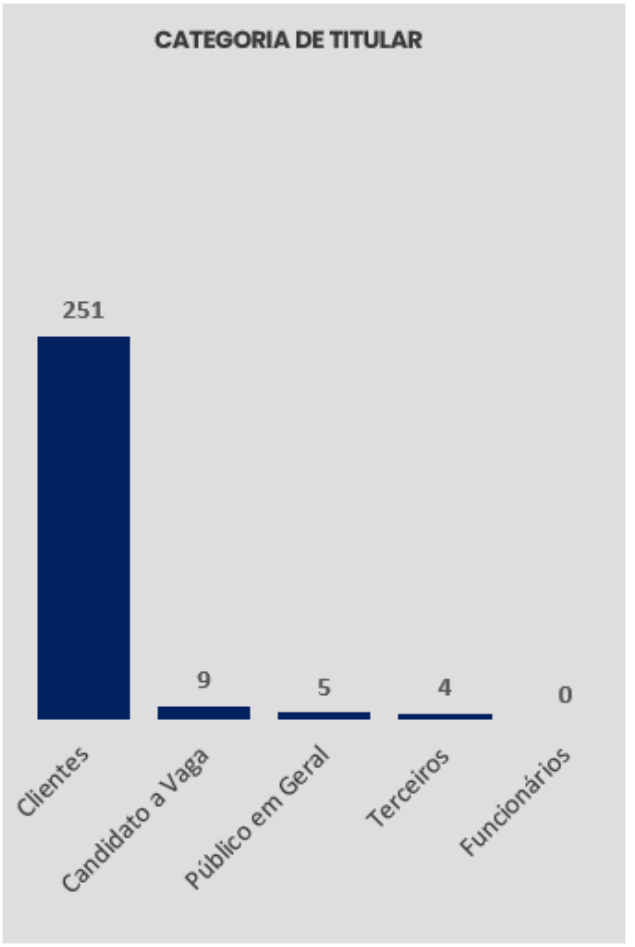
KPIs

- Avaliação de riscos de P&PD (due diligence)
- Contratos (adição da cláusula de P&PD)
- Pleito de titular (prazo de resposta)
- Consentimento
- Privacy by design & DPIA
- Teste de equilíbrio para legítimo interesse
- Extração de dados pessoais em massa
- Treinamentos e aviso de privacidade
- Execução dos planos de ação para mitigar riscos de privacidade

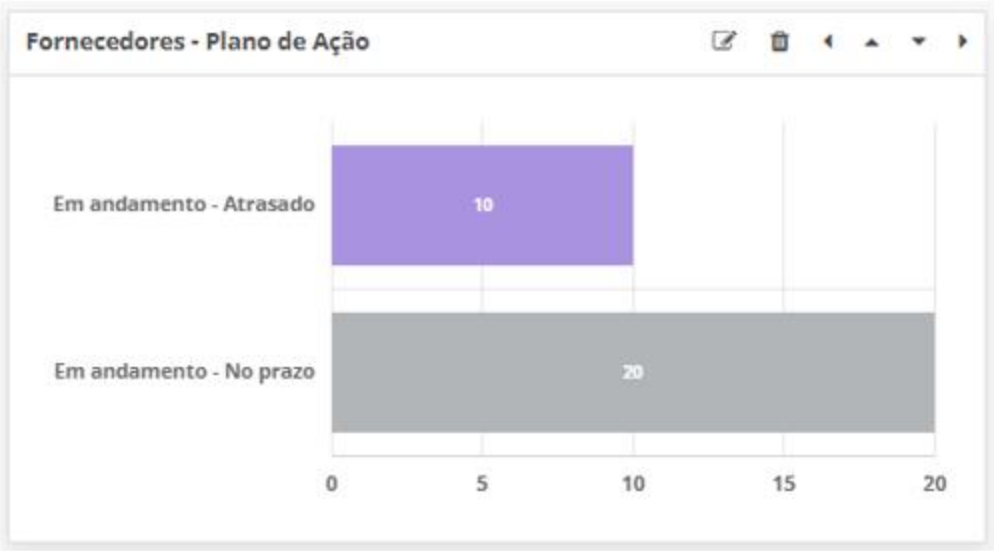
Exemplo de KPIs







Exemplo de KPIs

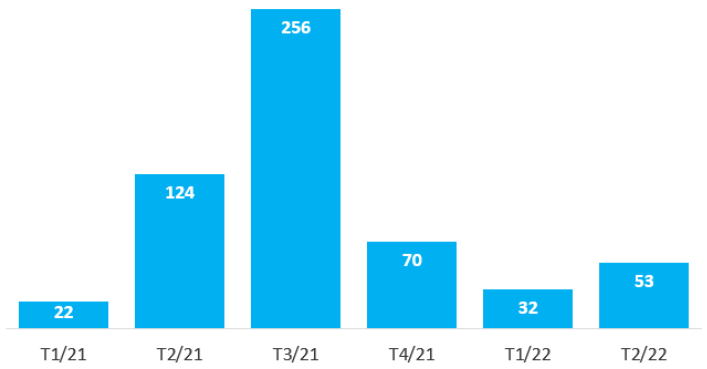


Em andamento - Atrasado

Nome	Organização	Tipo
AS GERENCIAMENTO E CONSULTORIA EIRELI	BRK	Desconhecido
Ille Engenharia Eireli	SPE Maranhão - Operação	Desconhecido
ALPA SEGURANCA DO TRABALHO LTDA	BRK	Operações
Iunes Advogados Associados	SPE Goiás - Comercial	Operações
APTA MED SERVICOS ESPECIALIZADOS EM MEDICINA E SEGURANCA DO T...	BRK	Desconhecido
BRANDALISE PORTALMED SST- SEGURANCA E SAUDE DO TRABALHO	BRK	Operações
EFFICO	SPE Recife - Comercial	Operações
CLINICA DE RADIOLOGIA IMAGEM CAÇADOR LTDA - DIGIMAX	SPE Caçador - QSSMA	Desconhecido
Gwm.net	BRK	Tecnologia
Laboratório de Analises Clinicas Madalozzo/Camati Ltda	SPE Caçador - QSSMA	Desconhecido

Exemplo de KPIs

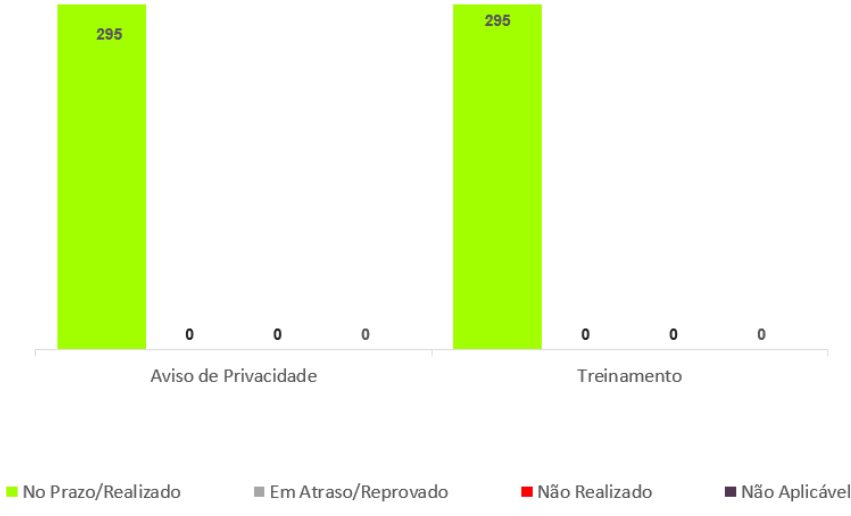
Privacy by Design



Status	Atividades
Concluída	51
Em andamento	2
Sob Revisão	0
Total	504

Em andamento	Atividades
Corporativo	2

Treinamentos e Aviso de Privacidade – novos empregados



295 FUNCIONÁRIOS ADMITIDOS NO PERÍODO

100% DOS AVISOS DE PRIVACIDADE ASSINADOS ANTES DA ADMISSÃO

100% DOS TREINAMENTOS REALIZADOS NO PRAZO

QUEBRA DE SEÇÃO

Subtítulo da apresentação

9º CONGRESSO INTERNACIONAL DE COMPLIANCE

9º CONGRESSO INTERNACIONAL DE COMPLIANCE

Siga a LEC nas redes sociais

@lecnews

@lec_news

@lec-news