



LGPD

IMPLANTAÇÃO
PERNAMBUCO

**APRESENTAÇÃO - CONTROLE
INTERNO**

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD (LEI 13.709/18)

Secretaria da
Controladoria
Geral do Estado

Regulamenta o tratamento dos dados pessoais por parte de entidades públicas e privadas.

- + DIREITOS**
- + CONTROLES**
- + TRANSPARÊNCIA**
- + RESPONSABILIDADE**
- + DEMANDAS**



LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

1	FINALIDADE	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
2	ADEQUAÇÃO	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
3	NECESSIDADE	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
4	ACESSO LIVRE	Garantia , aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
5	QUALIDADE DOS DADOS	Garantia , aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;



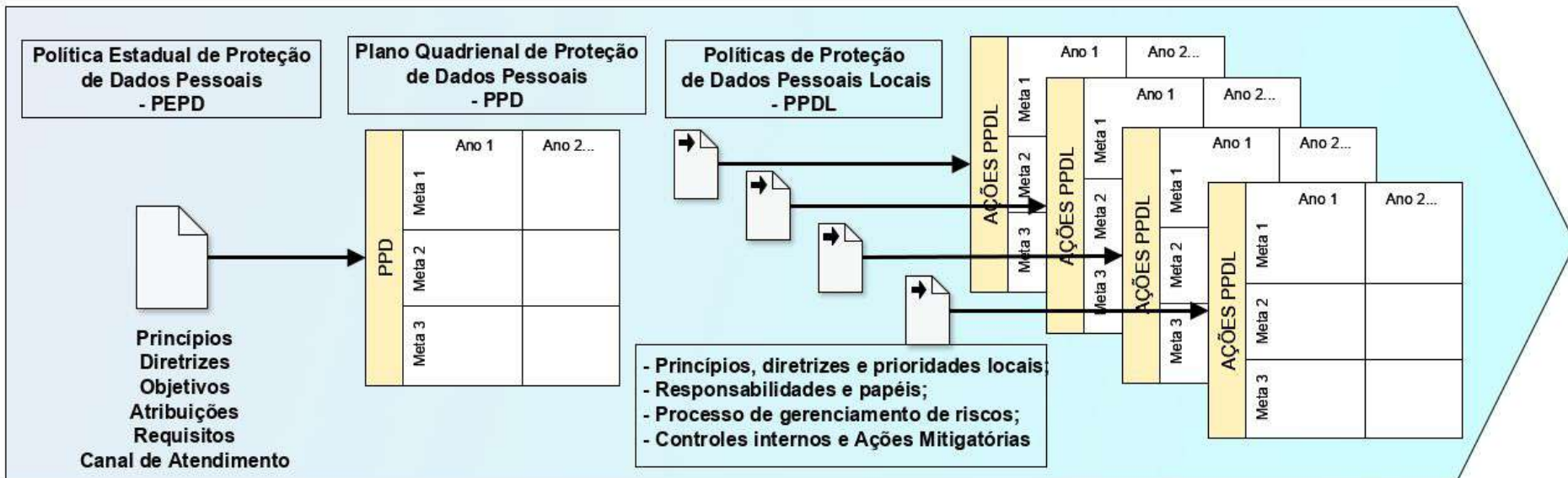
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

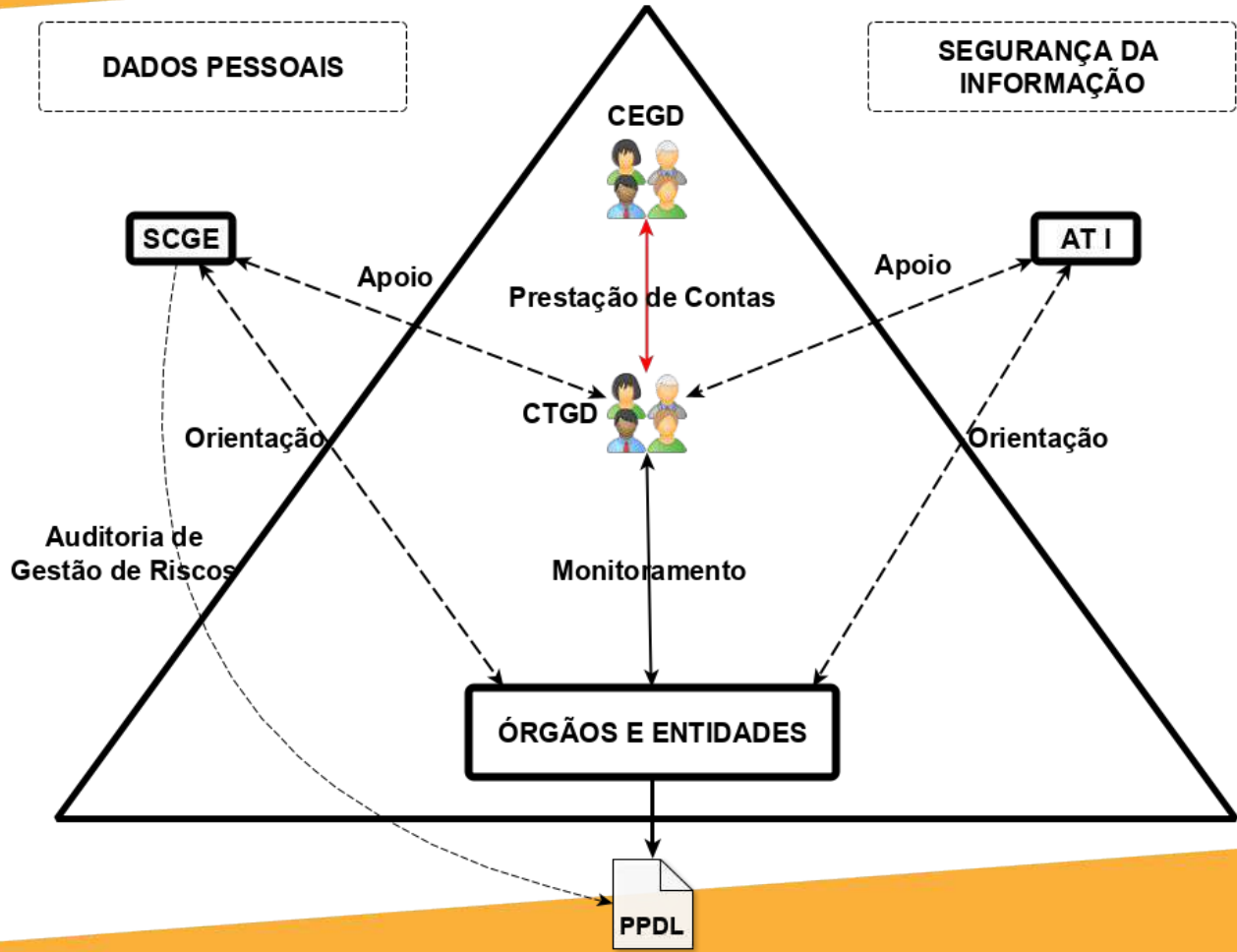
Secretaria da
Controladoria
Geral do Estado

6	TRANSPARÊNCIA	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento , observados os segredos comercial e industrial;
7	SEGURANÇA	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão ;
8	PREVENÇÃO	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
9	NÃO DISCRIMINAÇÃO	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos ;
10	ACCOUNTABILITY	Demonstração , pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive , da eficácia dessas medidas .



DECRETO ESTADUAL Nº 49.265/20





CANAL DE ATENDIMENTO



Secretaria da
Controladoria
Geral do Estado

GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO. MAIS FUTURO.



SUGESTÃO, RECLAMAÇÃO,
ELOGIO, SOLICITAÇÃO
E DENÚNCIA



CANAL DE
DENÚNCIAS
ANTICORRUPÇÃO



PEDIDO DE ACESSO
À INFORMAÇÃO
OU RECURSO



ACOMPANHAMENTO
DE PEDIDOS E
MANIFESTAÇÕES



CONSULTA PÚBLICA
DE PEDIDOS
E RECURSOS

Ouvidoria
Geral do Estado



MONITORAMENTO PEPD

PEPD

GESTÃO DE
RISCOS

$$R = P \times I$$

Risco

Probabilidade

Impacto

FAMÍLIA
ISO 27000
Segurança da Informação



MONITORAMENTO PEPD

05

NÍVEL

Gerenciamento em processos modelados e automatizados

04

NÍVEL

Gerenciamento em processos modelados

03

NÍVEL

Gerenciamento em macro-processos

02

NÍVEL

Gerenciamento de atribuições (Regulamento)

01

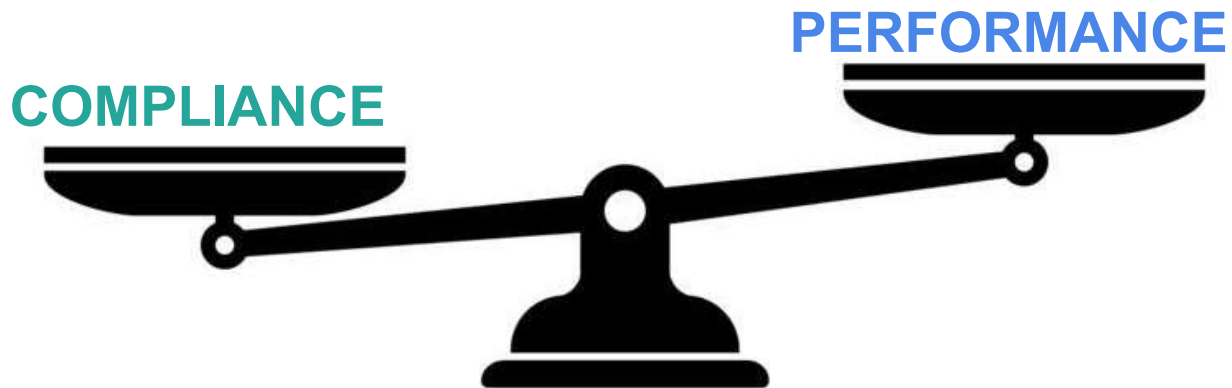
NÍVEL

Gerenciamento de atribuições (Lei)



MONITORAMENTO PEPD

Secretaria da
Controladoria
Geral do Estado



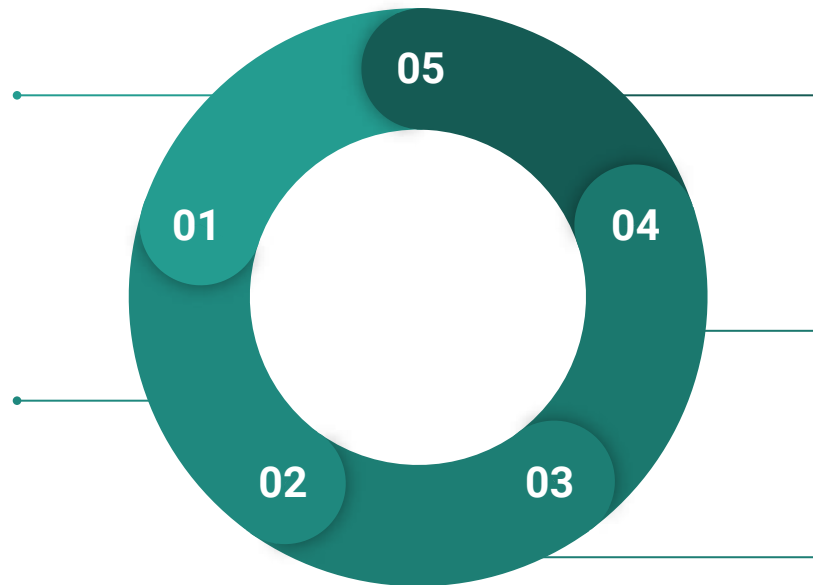
MONITORAMENTO - COMPLIANCE

Definição dos Pontos de Controle

Estabelecimentos da relação de pontos de controle por princípio com seus respectivos pontos.

Envio e Orientação

A SCGE irá enviar a todos os encarregados do Estado e estabelecerá um canal de apoio para orientação no preenchimento.



Auditoria Interna

A SCGE irá realizar periodicamente auditorias internas a fim de aferir a adequabilidade do gerenciamento de risco de compliance na LGPD

Apresentação dos Resultados Parciais de Compliance

A SCGE irá apresentar semestralmente os resultados parciais de adequação da LGPD ao CTGD para deliberações (alertas e orientações).

Aplicação da Auto-Avaliação de Compliance

Semestralmente as unidades de controle interno ou designado deverão realizar a auto-avaliação e enviá-la para SCGE.



MONITORAMENTO - COMPLIANCE

$$ICPD = (Pontuação\ atingida) \div (Pontuação\ máxima - Pontuação\ N/A)$$

EXEMPLO 01

- I. 10 pontos de controle
- II. Cada ponto de controle com pontuação igual a 10
- III. Auto-avaliação: SIM (8 pontos), NÃO (2 pontos)
- IV. Pontuação final: **80% = (80) ÷ (100 - 0)**

EXEMPLO 02

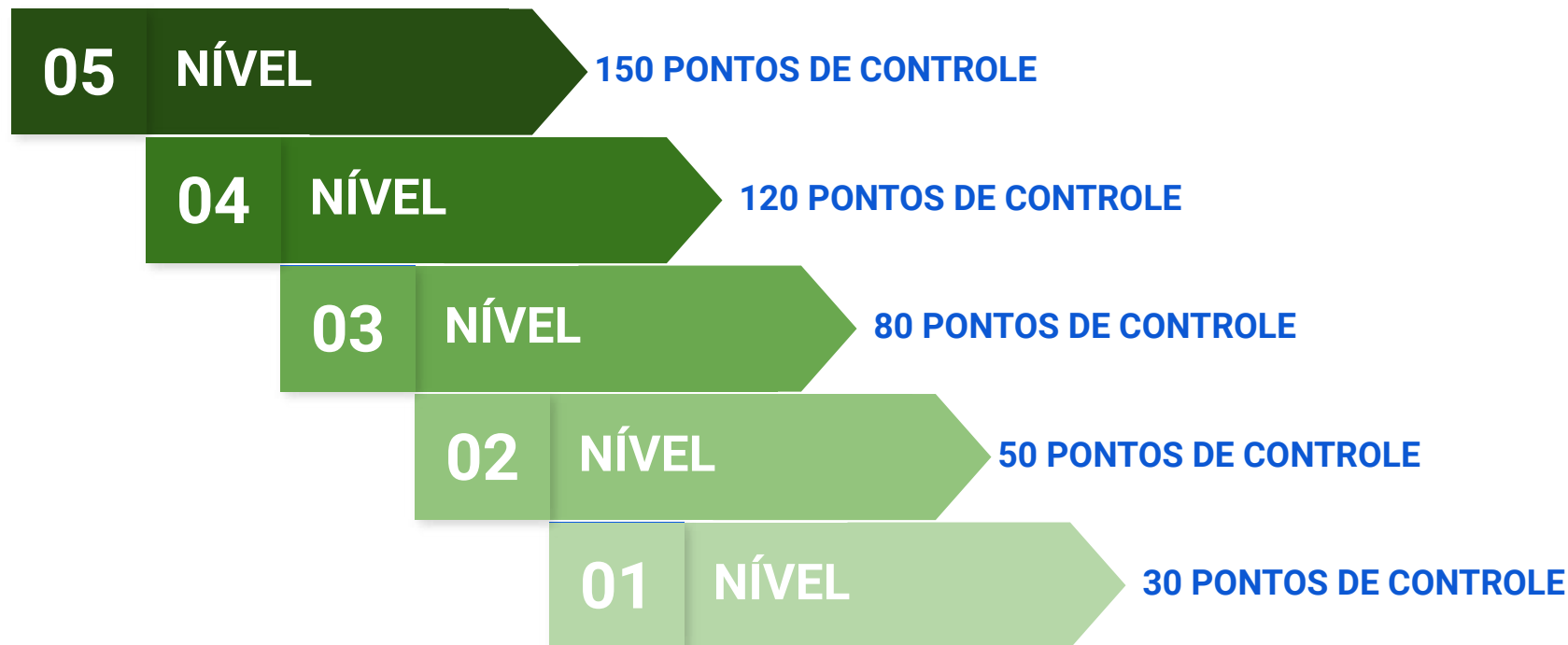
- I. 10 pontos de controle
- II. Cada ponto de controle com pontuação igual a 10
- III. Auto-avaliação: SIM (6 pontos), NÃO (2 pontos), N/A (2 pontos)
- IV. Pontuação final: **75% = (60) ÷ (100 - 20)**

Semestralmente, conforme Portaria, a SCGE consolidará os resultados. A partir do preenchimento da planilha, é gerado o ranking comparativo entre as unidades do Estado.

O ranking é então disponibilizado aos encarregados das unidades para que tenham a possibilidade de acompanhar sua evolução e de tomar medidas cabíveis a fim de manter ou melhorar seu índice. Cada encarregado só conseguirá visualizar a sua própria posição e a posição dos 3 primeiros colocados.



MONITORAMENTO - COMPLIANCE



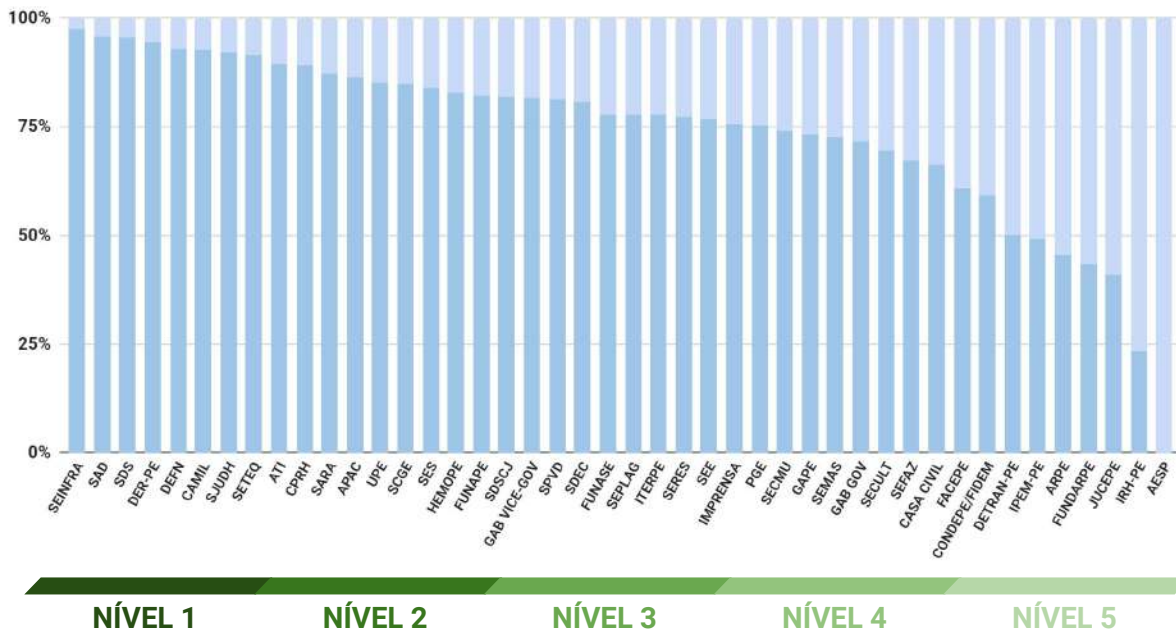
MONITORAMENTO - COMPLIANCE



Secretaria da
Controladoria
Geral do Estado

GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO. MAIS FUTURO.

Índice de Compliance de Proteção de Dados Pessoais - ICPD



COMPLIANCE LGPD





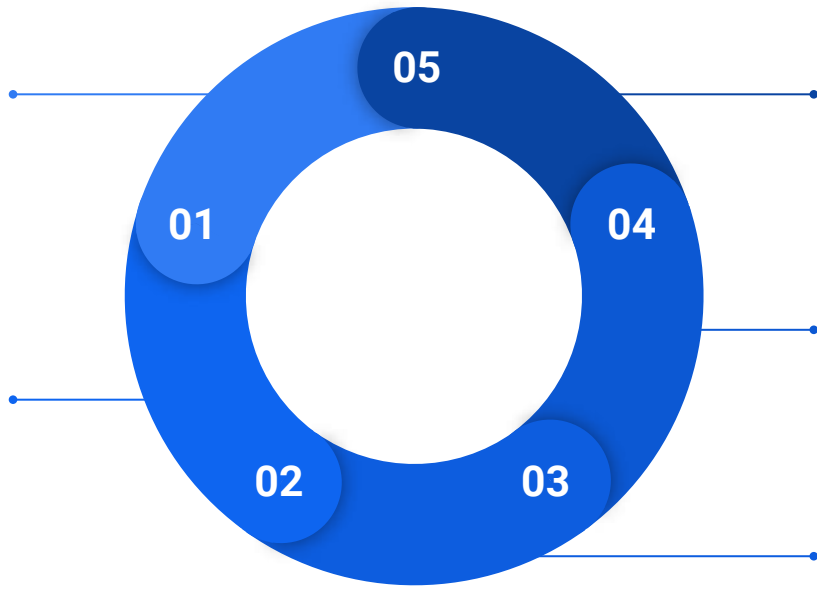
MONITORAMENTO - PERFORMANCE

Indicadores definidos em Portaria

Estabelecimentos da relação de indicadores de desempenho com a abertura de um canal de apoio para orientação no preenchimento.

Apuração dos Indicadores de Performance

Anualmente as unidades de controle interno ou designados deverão apurar os indicadores de desempenho e enviá-los para SCGE.



Apresentação dos Resultados Anuais de Performance - CEGD

A SCGE irá apresentar anualmente os resultados de performance e de compliance da LGPD considerando a proposta do CTGD e dos resultados das auditorias internas.

Apresentação dos Resultados Anuais de Performance - CTGD

A SCGE irá apresentar anualmente os resultados de performance da LGPD e os resultados das auditorias internas ao CTGD para montagem de proposta de avaliação .

Auditoria Interna

A SCGE irá realizar periodicamente auditorias internas a fim de aferir a adequabilidade do gerenciamento de risco de compliance na LGPD



MONITORAMENTO - PERFORMANCE

Painel Performance = Indicadores Desempenho + Indicadores Risco

Indicadores de Desempenho:

- a) Atualização e completude do Inventário de Dados Pessoais
- b) total de consultas efetuadas nos canais de atendimento da ouvidoria: principais controladores consultados, espécies de consulta, totais de atendimentos nas formas presencial e eletrônica;
- c) total detalhado das reclamações e queixas apresentados;
- d) total detalhado de respostas fora do prazo legal.



Indicadores de Risco:

- a) tratamentos com maior grau de risco;
- b) percentual de sistemas de informação que sofreram incidentes de segurança;
- c) principais espécies de incidentes de segurança, tempo de solução, e medidas adotadas.

GRC-PE



Monitora e apoia o projeto de implantação e execução da LGPD.

Comitê Privacidade

CONTROLADOR

Representante Legal

Aprova PPDPL, define prioridades, indica encarregado, emite instruções e presta contas.

OPERADOR

Operações

Órgãos, entidades, pessoas físicas e demais contratadas

ENCARREGADO

PPDPL

Gerencia projeto de implantação da LGPD e recomenda adequações.

Apoio Técnico

Ouvidoria e Controle Interno

- Transparência Ativa e Passiva
- Gestão de Riscos
- Compliance
- Accountability

Apoio jurídico

Jurídico

- Consulta e pareceres / LGPD
- Gestão do risco jurídico
- Proposições normativas

Apoio Tecnologia da Informação

Tec. da Informação

- Gestão de aplicações
- Gestão do Seg. da Informação
- Proposições técnicas



ENCARREGADO - DECRETO

1. **Inventariar os tratamentos** do controlador, inclusive os eletrônicos;
2. **Analisar a maturidade dos tratamentos** em face dos objetivos e metas estabelecidos e do conseqüente **risco de incidentes** de privacidade;
3. **Avaliar medidas de segurança, técnicas e administrativas** aptas a proteger os dados pessoais de **acessos não autorizados** e de **situações acidentais ou ilícitas** de destruição, perda, alteração, comunicação ou qualquer forma de **tratamento inadequado ou ilícito**;
4. **Adotar as providências cabíveis** para implementar as medidas de segurança avaliadas; e
5. **Cumprir os objetivos e metas** previstas na PPDPL.





EXEMPLO IMPLANTAÇÃO SCGE

Definição do Encarregado e Equipe de Apoio

Elaboração de Política de Proteção de Dados Local

Seminário de Conceitos Básicos e Instruções

Realização do Diagnóstico Preliminar

Entrevistas com Áreas Críticas

Inventário de Dados Pessoais

Elaboração e Aprovação do Plano de Adequação



IMPLANTAÇÃO EXEMPLO

- **Controlador:** SCGE;
- **Representação Legal:** Secretária da SCGE;
- **Comitê de Privacidade:** Conselho Deliberativo de Gestão - CDG;
- **Encarregado:** Assessoria Técnica - AST;
- **Equipe de apoio do encarregado:** Gerência de Assuntos Jurídicos - GAJ, Assessoria Especial de Controle Interno - AEI, a Ouvidoria da SCGE, a Diretoria de Tecnologia e Informação do Controle Interno - DTI e a Diretoria de Planejamento e Gestão - DPGE.
- **Gestor de Processos:** todo e qualquer responsável pela unidade de execução de um determinado processo de trabalho, inclusive sobre a gestão de riscos





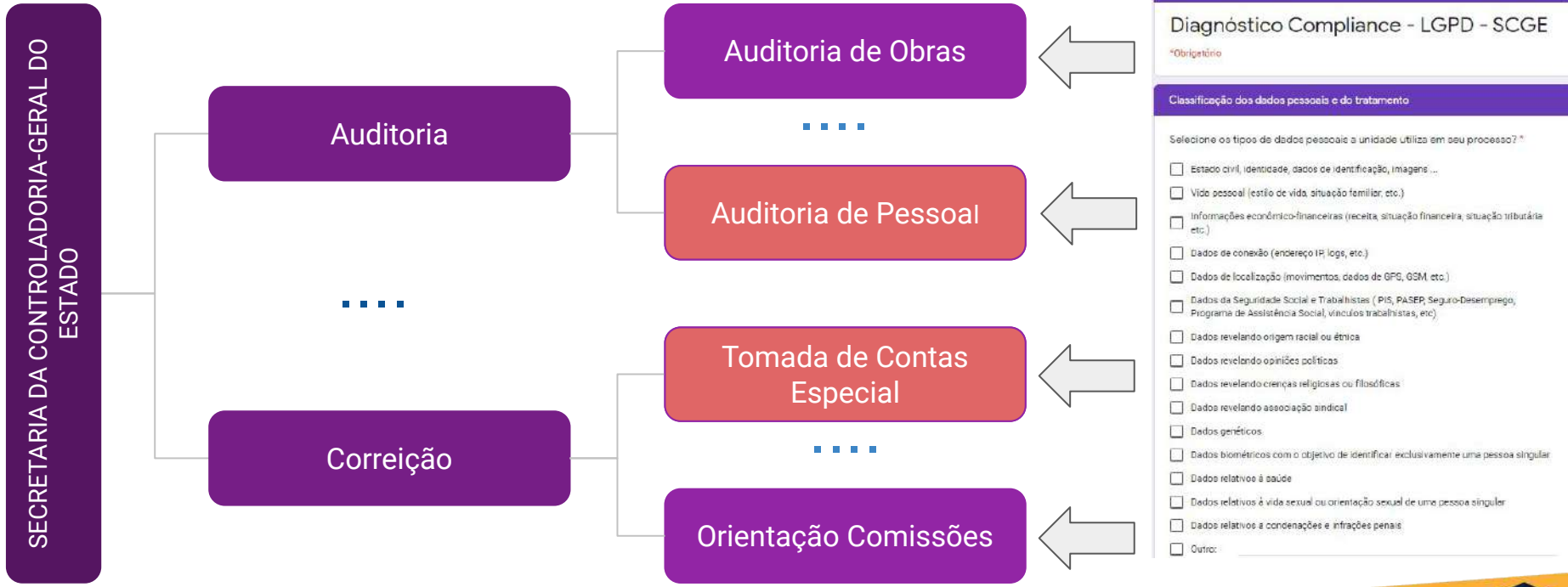
IMPLANTAÇÃO EXEMPLO - SEMINÁRIO

- Nível Estratégico;
- Conceitos Gerais LGPD;
- Decreto Estadual;
- Detalhes da Política de Proteção de Dados Pessoais Local;
- Instrução para o Diagnóstico Preliminar;
- Instrução para a Avaliação de Controles;
- Modelo de Inventário de Dados.





IMPLANTAÇÃO EXEMPLO - DIAGNÓSTICO



Diagnóstico Compliance - LGPD - SCGE

*Obrigatório

Classificação dos dados pessoais e do tratamento

Selecione os tipos de dados pessoais a unidade utiliza em seu processo? *

- Estado civil, identidade, dados de identificação, imagens ...
- Vida pessoal (estilo de vida, situação familiar, etc.)
- Informações econômico-financeiras (receita, situação financeira, situação tributária etc.)
- Dados de conexão (endereço IP, logs, etc.)
- Dados de localização (movimentos, dados de GPS, GSM, etc.)
- Dados da Seguridade Social e Trabalhistas (PIS, PASEP, Seguro-Desemprego, Programa de Assistência Social, vínculos trabalhistas, etc)
- Dados revelando origem racial ou étnica
- Dados revelando opiniões políticas
- Dados revelando crenças religiosas ou filosóficas
- Dados revelando associação sindical
- Dados genéticos
- Dados biométricos com o objetivo de identificar exclusivamente uma pessoa singular
- Dados relativos à saúde
- Dados relativos à vida sexual ou orientação sexual de uma pessoa singular
- Dados relativos a condenações e infrações penais
- Outros: _____





IMPLANTAÇÃO EXEMPLO

Avaliação de Controles - Ações Corretivas

Já houve algum incidente de acesso indevido? *

- Sim
 Não

Caso tenha ocorrido o incidente de acesso indevido, a unidade orientou o funcionário?

- Sim
 Não

Na ocorrência de comunicação irregular, a unidade tem como informar qual o é funcionário responsável? *

- Sim
 Não

Avaliação de Controles - Ações Preventivas

Qual procedimento a unidade adota para atualizar o acesso no ingresso ou saída do funcionário? *

Sua resposta

Os funcionários são orientados sobre a segurança dos dados? Caso positivo, descreva como. *

Sua resposta

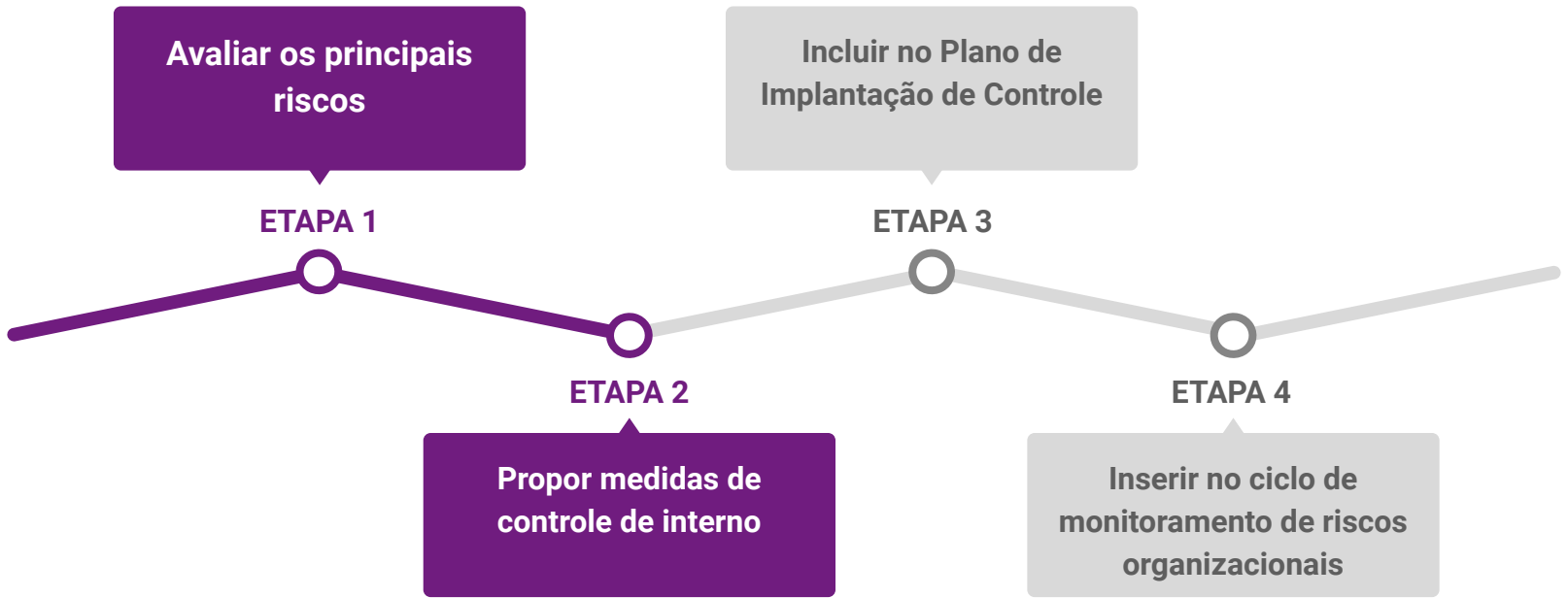
A unidade admite o compartilhamento de dados através de mídia externa ou nuvem? Caso positivo, descreva a finalidade *

Sua resposta





IMPLANTAÇÃO EXEMPLO



IMPLANTAÇÃO EXEMPLO

R	Responsável
A	Aprovador
C	Consultado
I	Informado

Secretaria da
Controladoria
Geral do Estado

MATRIZ RACI SCGE - PROCESSO DE IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD

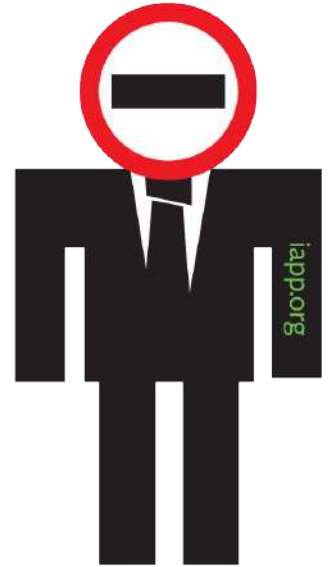
Atividade\Estrutura	Secretária	CDG	Encarregado	AECI	GAJ	DTCI	DPGE	Ouvidoria	Gestor de Processo
PPDPL	A	C	R	C	C	C	C	C	-
Sensibilização	-	-	R	-	-	-	-	-	-
Diagnóstico Preliminar	I	I	C/A/I	R	-	R	-	-	R
Avaliação de Controles	I	I	C/A/I	R	-	R	-	-	R
Proposta de ações	-	-	C/A/I	C	-	C	-	C	R
Plano de Implementação de Controles	A	C	R	C	I	I	I	I	I
Monitoramento PPDPL	I	I	R	C	C	C	-	-	R
Atendimento Titular	-	I	A	I	C	R	-	R	R
Inventário de Dados	A	C	R	C	-	R	-	I	R
Ajustes Contratuais	A	I	C/I	I	R	C	R	-	-
Plano de Incidentes	A	C	R	C	C	C	C	-	C
Relatório de Impacto	A	C	R	C	C	C	-	I	C
Elaboração de Termos de Uso e Termos de Consentimento	-	-	C	C	R	C	C	-	C
Transparência dos tratamentos de Dados	-	I	C	I	I	C	-	R	I
Tabela de Prazos de Retenção de Dados	-	-	C	-	C	C	R	-	C





PRÓXIMOS PASSOS

- Portaria de Monitoramento PEPD;
- Portaria de Orientações e Controles Padrões;
- Portaria Atendimento - Ouvidoria;
- Plano Quadrienal Estratégico de Proteção de Dados Pessoais.



PRIVACY
Like A **BOSS**



Secretaria da
Controladoria
Geral do Estado



GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO, MAIS FUTURO.