ADEQUAÇÃO À LEI GERAL DE

AVALIAÇÃO DE RISCOS DE SI&P

LGPD PERNAMBUCO

Secretaria da Controladoria Geral do Estado

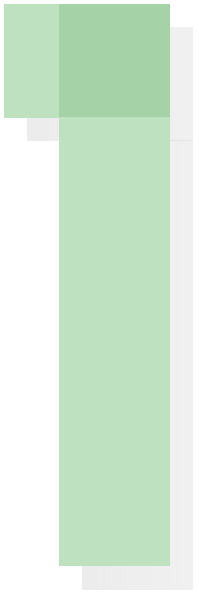
GOVERNO DE PERNAMBUCO ESTADO DE MUDANÇA

Política Estadual de Segurança da Informação

Decreto nº 49.914, de 10 de dezembro de 2020

Art. 5º São diretrizes gerais da Política Estadual de Segurança da Informação - PESI: (...)

V - implantar o processo de gestão de riscos de Tecnologia da Informação e Comunicação - TIC, para análise periódica e sistemática do impacto na área de negócio;



Premissas da Metodologia

MODELO - CGE-PE

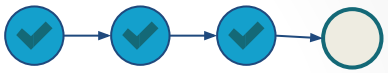
Metodologia de Gerenciamento de Riscos de SI&P

- Adaptação do Modelo de Gestão de riscos da Governo Digital da União
- Integrado ao Modelo de Gestão de riscos da SCGE-PE
- Voltado para Processos de Negócio que estejam mapeados
- Nível de Risco calculado em função da avaliação dos controles internos
- Gerenciamento “de cima para baixo”
- Escopo baseado no Método de Priorização de Processos

LGPD
PERNAMBUCO

Avaliação de Riscos de SI&P - Premissas

O que fazer antes de iniciar a ação de gerenciamento de Riscos de SI&P



Mapeamento dos Processos do Escopo de Avaliação de Riscos de SI&P

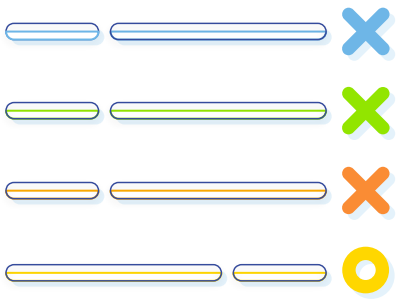
Inventário de Dados Pessoais do Escopo de Avaliação de Riscos de SI&P

Gestão de Riscos
SCGE-PE

Realização do Curso de Gerenciamento de Riscos CGE-PE / CEFOSPE

Leitura do Manual de Gerenciamento de Riscos de SI&P CGE-PE

Avaliação de Riscos de SI&P - Premissas



Questionário de Avaliação de

Riscos de SI&P

Modelo CGE PE

A mensuração do Risco se dá através da avaliação por meio de um questionário que apura a existência (ou não) de 66 controles e a sua aplicação nos processos do Escopo. Estes controles estão associados a 14 eventos de risco previstos

Avaliação de Riscos de SI&P - Premissas

Os controles são classificados de acordo com a forma de atuação no Risco, sendo divididos em:

 # Controles Preventivos

 # Controles Mitigatórios

 # Controles Mistos

Os controles são avaliados de acordo com a utilidade e relevância para o Risco

 # Não se aplica ao Risco: 0,0

 # Aplica-se ao risco: 5,0

 # Aplica-se e é Prioritário: 10,0

Avaliação de Riscos de SI&P - Premissas

ID	Risco	Controles "Preventivos"	Controles "Mitigatórios"	Controles "Mistos"	Total de Controles aplicáveis ao Risco
01	Acesso não autorizado	35	04	11	50
02	Coleção excessiva	9	-	3	12
03	Compartilhamento / distribuição de Dados Pessoais sem o consentimento do titular dos dados pessoais	8	-	1	09
04	Falha em considerar os direitos do titular dos dados pessoais	23	05	2	30
05	Falha ou erro de processamento	7	05	1	13
06	Informação insuficiente sobre a finalidade do tratamento	7	01	1	09
07	Modificação não autorizada	33	06	13	52
08	Perda	27	12	14	53
09	Reidentificação de dados pseudo minimizados	8	-	1	09
10	Remoção não autorizada	32	04	14	50
11	Retenção prolongada de dados pessoais sem necessidade	7	01	2	10
12	Roubo	27	06	21	54
13	Tratamento sem consentimento do titular dos dados pessoais	12	-	3	15
14	Vinculação ou associação indevida direta ou indireta dos dados pessoais ao titular	16	-	5	21

Avaliação de Riscos de SI&P - Premissas

ID	Risco	Pontuação dos Controles		
		"Aplicáveis"	"Prioritários"	Total
01	Acesso não autorizado	18	32	410
02	Coleção excessiva	03	9	105
03	Compartilhamento / distribuição de Dados Pessoais sem o consentimento do titular dos dados pessoais	01	8	85
04	Falha em considerar os direitos do titular dos dados pessoais	20	10	200
05	Falha ou erro de processamento	07	6	95
06	Informação insuficiente sobre a finalidade do tratamento	07	2	55
07	Modificação não autorizada	11	41	465
08	Perda	15	38	455
09	Reidentificação de dados pseudo minimizados	02	7	80
10	Remoção não autorizada	04	46	480
11	Retenção prolongada de dados pessoais sem necessidade	06	4	70
12	Roubo	05	49	515
13	Tratamento sem consentimento do titular dos dados pessoais	05	10	125
14	Vinculação ou associação indevida direta ou indireta dos dados pessoais ao titular	06	15	180

Avaliação de Riscos de SI&P - Premissas

03
Dimensões

Todas as dimensões tratam os temas Segurança e Privacidade, mas dentro do contexto de cada dimensão

24
Estrutura

Controles que tratam de **aspectos estruturais do sistema (processos e infraestrutura que o sustentam)**, características de ambiente que expandem a análise, mas indispensável para identificar o estado atual da segurança e privacidade na organização responsável pelo tratamento de dados pessoais

25
Sistema

A dimensão Sistema tem alicerce no processo de Security-by-Design, ou seja, os controles de segurança propostos visam **incorporar a segurança da informação durante todo o ciclo de vida do sistema**, consequentemente auxiliam a redução da superfície de ataque para vulnerabilidades de sistema

17
Privacidade

Controles relacionados ao **alcance da conformidade legal com à privacidade** de tratamento de dados pessoais. Os controles permitirão que o controlador analise o sistema que trata dados pessoais e verifique se os requisitos de adequação à privacidade estão sendo atendidos.

Avaliação de Riscos de SI&P - Premissas

Os controles previstos são também analisados de acordo com seus objetivos, de maneira que cada um dos 66 controles podem ser divididos em duas categorias:

- Medidas de Segurança
  - 1 Continuidade de Negócio
  - 2 Controles Criptográficos
  - 3 Controles de Acesso Lógico
  - 4 Controles de Seg. Redes, Proteção Física / do Ambiente
  - 5 Cópia de Segurança
  - 6 Desenvolvimento Seguro
  - 7 Gestão de Capacidade e Redundância
  - 8 Gestão de Mudanças
  - 9 Gestão de Riscos
  - 10 Reg. de Eventos, Rastreabilidade e Salvaguarda de Logs
  - 11 Resposta a Incidente
  - 12 Segurança Web
- Medidas de Privacidade
  - 1 Abertura, Transparência e Notificação
  - 2 Compliance com a Privacidade
  - 3 Consentimento e Escolha
  - 4 Controles de Acesso e Privacidade
  - 5 Legitimidade e Especificação de Propósito
  - 6 Limitação da Coleta
  - 7 Minimização dos Dados
  - 8 Participação Individual e Acesso
  - 9 Precisão e Qualidade
  - 10 Responsabilização
  - 11 Uso, retenção e Limitação e Divulgação

LGPD PERNAMBUCO

Avaliação de Riscos de SI&P - Premissas

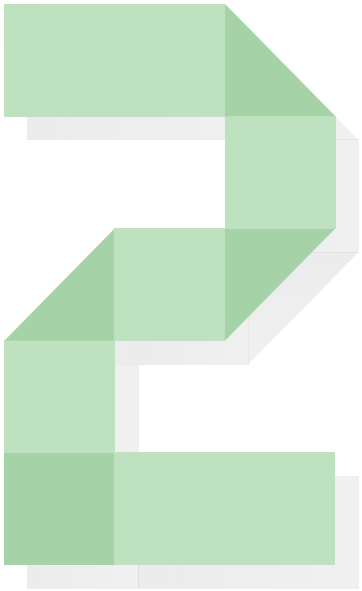
ID	MEDIDA DE SEGURANÇA	OBJETIVO DOS CONTROLES ASSOCIADOS À MEDIDA
1	Continuidade de Negócio	Manter a operação da atividade, apesar das adversidades enfrentadas
2	Controles Criptográficos	Oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento)
3	Controles de Acesso Lógico	Limitar os acessos indevidos ao sistema
4	Controles de Segurança em Redes, Proteção Física e do Ambiente	Evitar acessos indevidos às estruturas internas
5	Cópia de Segurança	Realizar e manter cópias com temporariedade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais
6	Desenvolvimento Seguro	Atender critérios de segurança da informação, desde a concepção do produto
7	Gestão de Capacidade e Redundância	Manter a disponibilidade do serviço
8	Gestão de Mudanças	Acompanhar as mudanças, comunicar aos interessados e identificar potenciais riscos
9	Gestão de Riscos	Identificar, avaliar, gerenciar e monitorar os riscos identificados
10	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	Registrar eventos com atributos de rastreabilidade e proteger de alteração e acessos indevidos
11	Resposta a Incidente	Realizar a coleta, a preservação de evidências, o tratamento e a resposta a incidentes de segurança
12	Segurança Web	Elevar os níveis de segurança (da camada de front-end) nos serviços de acessos eletrônicos

Avaliação de Riscos de SI&P - Premissas

ID	MEDIDA DE PRIVACIDADE	OBJETIVO DOS CONTROLES ASSOCIADOS À MEDIDA
1	Abertura, Transparência e Notificação	Atender o princípio de transparência da LGPD (Art. 6°, inciso VI)
2	Compliance com a Privacidade	Atender a legislação de proteção de dados, monitorar e auditar a privacidade
3	Consentimento e Escolha	Obter consentimento do titular (Art. 7°, I) desde que não se enquadre nas demais hipóteses previstas pelo art. 7° e 11 da LGPD
4	Controles de Acesso e Privacidade	Limitar acessos indevidos às operações de tratamento de dados pessoais (LGPD, art. 6°, Incisos VII e VIII)
5	Legitimidade e Especificação de Propósito	Realizar tratamento para propósitos legítimos, específicos explícitos e informados ao titular (LGPD, art. 6°, I)
6	Limitação da Coleta	Limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6°, III)
7	Minimização dos Dados	Minimizar os dados utilizados no processamento (LGPD, art. 6°, III)
8	Participação Individual e Acesso	Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6°, IV)
9	Precisão e Qualidade	Assegurar que os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento (LGPD, art. 6°, V)
10	Responsabilização	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de DP (LGPD, art. 6°, X)
11	Uso, retenção e Limitação e Divulgação	Assegurar aos titulares os direitos fundamentais de liberdade, de intimidade e de privacidade ao realizar o tratamento de DP

Avaliação de Riscos de SI&P - Premissas

OBS: 14 eventos de risco propostos pelo Comitê Central de Governança de Dados da União - CCGD que foram influenciados e adaptados da norma ISO/IEC 29134:2017.



Cálculo do Risco

MODELO - CGE-PE

Avaliação de Riscos de SI&P - Premissas

Nível de Risco

Probabilidade de Ocorrência

Impacto da Materialização

Avaliação de Riscos de SI&P - Premissas

Para calcular a probabilidade de ocorrência do Risco, deve-se inicialmente calcular o percentual de atendimento das medidas de controles preventivos e mistos, conforme descrito a seguir:

Conforme pode ser deduzido da fórmula acima, se todos os controles forem aplicados no processo em análise, então o valor encontrado será 1 (um). Em oposição, se nenhum controle for aplicado, então o valor final será 0 (zero).

Avaliação de Riscos de SI&P - Cálculo do Risco

$$\text{\% Atendimento dos Controles de Prevenção} = \frac{\text{Pontuação Alcançada dos Controles Preventivos}}{\text{Pontuação Possível dos Controles Preventivos}}$$

PONTUAÇÃO ALCANÇADA	PONTUAÇÃO POSSÍVEL
Total de pontos dos controles preventivos e Mistos cuja resposta atribuída foi "SIM"	*(Total de pontos dos Controles Preventivos e Mistos associados ao Risco)* - *(Total de pontos dos controles Preventivos e Mistos cuja resposta atribuída foi "NÃO SE APLICA")*

Probabilidade = 10 - (% Atendimento dos Controles de Prevenção x 10)

Em seguida, a probabilidade do evento de risco é calculada por meio da aplicação da equação acima. Importante destacar que a nota estimada da probabilidade considera uma escala de 0 (zero) a 10 (dez), em que 0 (zero) corresponde à nota mínima possível para a probabilidade de ocorrência de um evento de risco e 10 (dez) à nota atribuível para os eventos cuja probabilidade de ocorrência é máxima

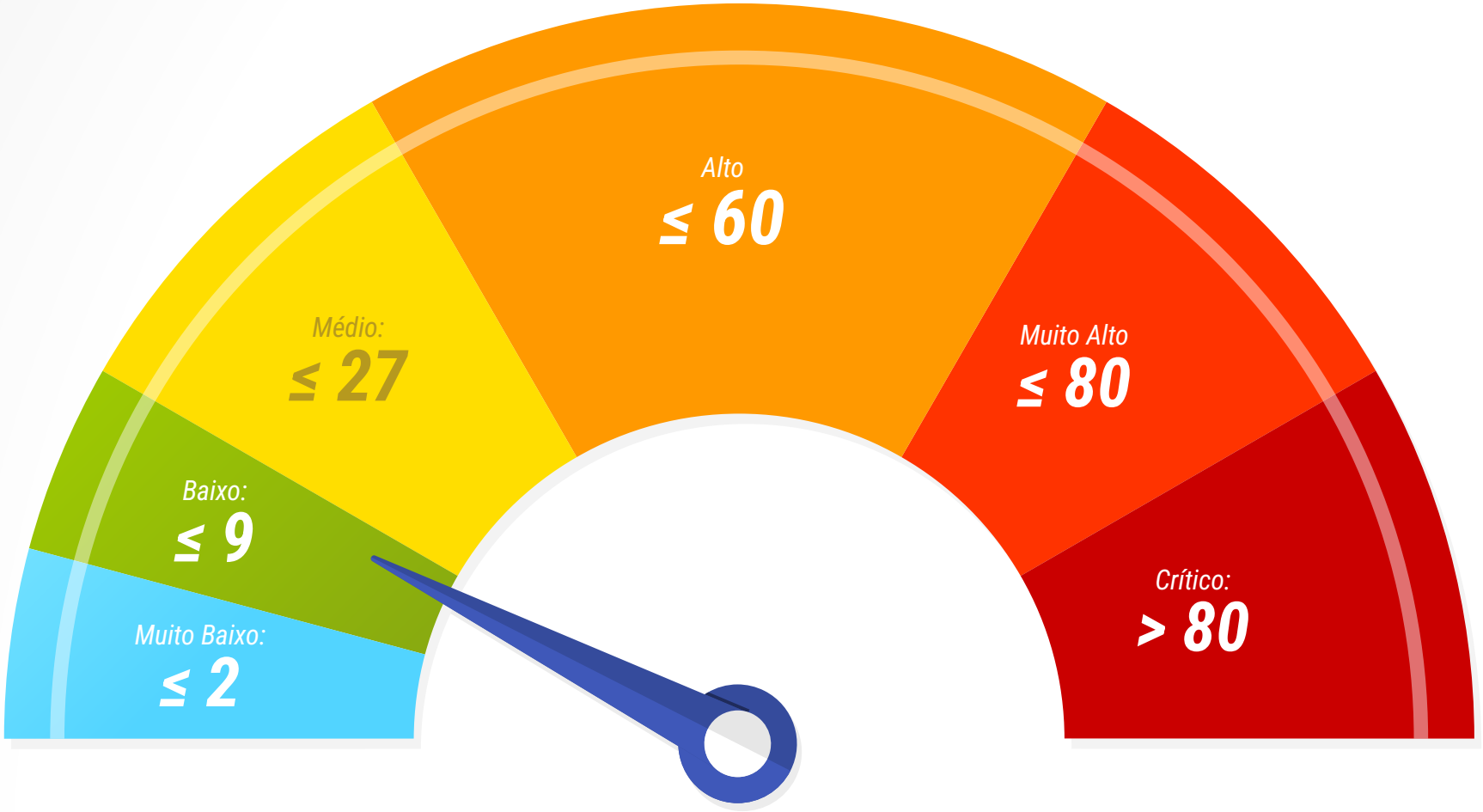
ATENÇÃO: *O cálculo do impacto segue a mesma lógica explicada para a aferição da Probabilidade*

Avaliação de Riscos de SI&P - Cálculo do Risco

PROBABILIDADE		
PROBABILIDADE	NOTA	VULNERABILIDADE
MUITO BAIXA	1	Evento raro. Em situações excepcionais, o evento poderá até ocorrer, mas nem o histórico, nem as circunstâncias indicam essa possibilidade.
BAIXA	2	Evento improvável. De forma inesperada ou casual, o evento poderá ocorrer, mas o histórico e as circunstâncias pouco indicam essa possibilidade.
MÉDIA	5	Evento possível. De alguma forma, o evento poderá ocorrer, pois o histórico e as circunstâncias indicam moderadamente essa possibilidade.
ALTA	8	Evento provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
MUITO ALTA	10	Evento esperado. Exceto em situações excepcionais, o evento deve ocorrer, pois as circunstâncias indicam claramente essa possibilidade.

IMPACTO		
IMPACTO	NOTA	VULNERABILIDADE
MUITO BAIXO	1	Impacto nulo ou insignificante, comprometendo minimamente o alcance do objetivo/resultado, com mínima necessidade de recuperação.
BAIXO	2	Impacto pouco relevante, comprometendo em alguma medida o alcance do objetivo/resultado, com pequena necessidade de recuperação.
MÉDIO	5	Impacto relevante, comprometendo moderadamente o alcance do objetivo/resultado, com razoável necessidade de recuperação.
ALTO	8	Impacto muito relevante, comprometendo significativamente o alcance do objetivo/resultado, mas com possibilidade de recuperação.
MUITO ALTO	10	Impacto catastrófico, comprometendo total ou quase totalmente o alcance do objetivo/resultado, com remota ou nenhuma possibilidade de recuperação.

Avaliação de Riscos de SI&P - Níveis de Risco (Modelo CGE-PE)



Avaliação de Riscos de SI&P - Exemplo

RISCO	PONTUAÇÃO - PREVENTIVOS			PONTUAÇÃO - MITIGATÓRIOS			PONTUAÇÃO - MISTOS		
	POSSÍVEL	ALCANÇADA	N/A	POSSÍVEL	ALCANÇADA	N/A	POSSÍVEL	ALCANÇADA	N/A
1	295	65	10	20	0	0	95	10	0
2	80	30	0	0	0	0	25	15	0
3	75	20	0	0	0	0	10	10	0
4	150	35	0	35	0	0	15	15	0
5	50	20	0	35	0	0	10	10	0
6	40	20	0	10	0	0	05	05	0
7	285	60	10	55	0	10	125	10	0
8	215	50	10	115	0	0	125	15	0
9	70	15	0	0	0	0	10	10	0
10	305	75	10	35	0	0	140	10	0
11	50	10	0	10	0	0	10	10	0
12	260	70	10	55	0	0	200	15	0
13	100	25	0	0	0	0	25	10	0
14	130	25	0	0	0	0	40	15	0

PREFEITURA DA CIDADE
RIACHO DO NAVIO
Secretaria de Saúde

- EXEMPLO -

Gerenciamento de Riscos de SI&P do Processo de Concessão de Licenças e Afastamentos de servidores efetivos e comissionados da Secretaria de Saúde da Prefeitura de Riacho do Navio

Avaliação de Riscos de SI&P - Exemplo

Risco nº04

"Falha em considerar os direitos do titular dos dados pessoais"

Descrição: Compartilhar ou Distribuir Dados Pessoais sem o consentimento do Titular dos dados pessoais

RA = Risco Alto

1º	% Atendimento dos Controles de Prevenção	$= \frac{50}{(150-0)+(15-0)}$	= 0,3030
2º	Avaliação da Probabilidade	= 10 - (0,3030 x 10)	= 6,969
3º	% Atendimento dos Controles de Mitigação	$= \frac{15}{(35-0)+(15-0)}$	= 0,3000
4º	Avaliação do Impacto	= 10 - (0,3000 x 10)	= 7,000

Nível do Risco = 6,969 x 7,000 = 48,783

Avaliação de Riscos de SI&P - Exemplo

Risco nº07

"Modificação não autorizada"

Descrição: Usuários sem permissão de alteração para determinado DP ou registro realiza modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.

RMA = Risco Muito Alto

1º % Atendimento dos Controles de Prevenção = $\frac{(60 + 10)}{(285-10) + (125-0)}$ = 0,1750

2º Avaliação da Probabilidade = 10 - (0,1750 x 10) = 8,250

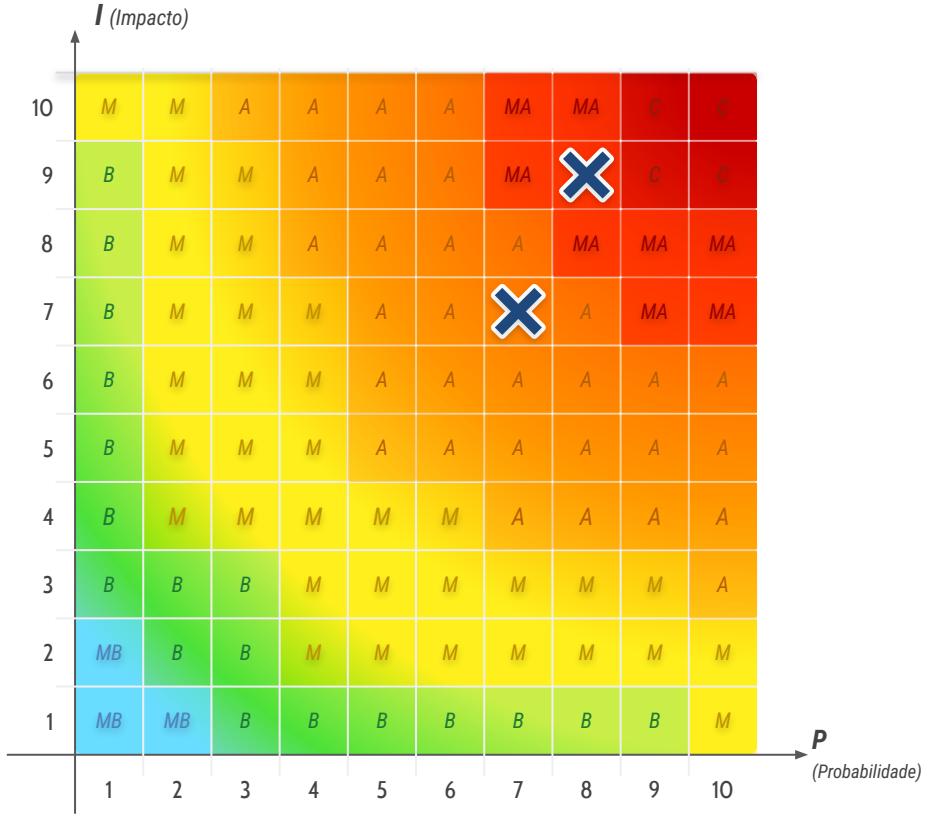
3º % Atendimento dos Controles de Mitigação = $\frac{(0 + 10)}{(55-10) + (125-0)}$ = 0,0588

4º Avaliação do Impacto = 10 - (0,3000 x 10) = 9,412

Nível do Risco = 8,250 x 9,412 = 77,649

Avaliação de Riscos de SI&P - Exemplo

RISCO MUITO BAIXO	≤ 2
RISCO BAIXO	≤ 9
RISCO MÉDIO	≤ 27
RB - RISCO ALTO	≤ 60
RISCO MUITO ALTO	≤ 80
RISCO CRÍTICO	> 80



Avaliação de Riscos de SI&P - Material de Apoio

Política

Manual

Planilha de Trabalho

Modelo de Gestão de Riscos Corporativos - SCGE PE

Planejamento → **Implantação** → Monitoramento → Revisão

PASSO 01
Contexto e Escopo

PASSO 02
Identificação dos Riscos

PASSO 03
Avaliação dos Controles

PASSO 04
Definição do Risco Residual

PASSO 05
Validação do Risco Inerente

PASSO 06
Definição das Respostas

PASSO 07
Elaboração do Plano de Tratamento

Avaliação de Riscos de SI&P

PASSO 01

Contexto e Escopo

- Questionário: Diagnóstico Preliminar
- Planilha de Priorização de Processo
- Modelo de Mapeamento de Processos

PASSO 02

Identificação dos Riscos

- Listagem de Eventos de Risco
- Inventário de Dados Pessoais (BI)
- Tabela de Tratamento de Dados

PASSO 03

Identificação dos Controle

- Questionário de Avaliação dos Controles

PASSO 04

Definição do Risco Residual

- Planilha de Gerenciamento de Riscos

PASSO 05

Validação do Risco Inerente

PASSO 06

Definição das Respostas

PASSO 07

Elaboração do Plano Tratamento

- Plano de Tratamento
- RIPD

Referências Teóricas:

- ISO/IEC 27002:2013: Código de prática para controles de segurança da informação
- ISO/IEC 29134:2017: Avaliação de Impacto de Privacidade
- ISO/IEC 29100:2011: Estrutura de Privacidade

Diretoria de Tecnologia da Informação do Controle Interno

Coordenadoria de Proteção de Dados Pessoais

- Diretora: Sandra Lubambo
- Coordenador: Pedro Hilário
- Equipe técnica: Karlos Aragão

LGPD PERNAMBUCO

Secretaria da Controladoria Geral do Estado

GOVERNO DE PERNAMBUCO ESTADO DE MUDANÇA

LGPD
PERNAMBUCO

lgpd@cge.pe.gov.br