PLANO DE ANÁLISE DE RISCOS

DISTRIBUIDORA DE FILMES S.A. - RIOFILME

Plano de Análise de Riscos

DESCRIÇÃO DO RISCO	FUNDAMENTAÇÃO DO RISCO	PROBABILIDADE DO RISCO	IMPACTO DO RISCO	NÍVEL DE RISCO (P x I)	CLASSIFICAÇÃO DO RISCO	AÇÕES PARA MITIGAÇÃO DO RISCO	RISCO RESIDUAL
Detalhar o risco relativo ao cumprimento das normas e boas práticas de proteção de dados pessoais	*Mencionar a norma legal ou boa prática (ISO, etc) que pode ser violada*	*Elencar a probabilidade de ocorrência do risco em uma escala 5 -10 - 15*	*Elencar o impacto de ocorrência do risco em uma escala 5 -10 - 15*		Alto / Médio / Baixo	*Indicar ações sugeridas para tratar o risco*	*Alto / Médio / Baixo*
Ausência de indicação de encarregado	Art. 41, LGPD	15	15	225	Alto	indicar encarregado pelo tratamento dos dados pessoais, disponibilizar o contato com o encarregado	Baixo
Acesso não autorizado	princípio da segurança (art. 6, VII e art. 46, LGPD) + ISO / IEC 29134:2017	15	15	225	Alto	política de credenciais; controle de acesso lógico; política de segurança em redes; restrição de acesso aos arquivos físicos	Médio
Modificação não autorizada	princípio da segurança (art. 6, VII e art. 46, LGPD) + ISO / IEC 29134:2017	10	15	150	Alto	política de credenciais; controle de acesso lógico; política de segurança em redes; termo de responsabilidade	Médio
Tratamento sem consentimento do titular dos dados pessoais (Caso a base legal seja consentimento)	Art 5, inciso XII e art. 7, inciso I, LGPD	10	15	150	Alto	termo de consentimento; mapeamento de dados pessoais	Baixo

Compartilhar ou distribuir dados pessoais com terceiros fora das hipóteses de compartilhamento	Art. 26 e 27 da LGPD	10	15	150	Alto	termo de uso; contratos com cláusulas destacadas acerca da transferência de dados pessoais, especificando a base legal	Baixo
Perda	princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD)	10	10	100	Médio	política de resposta de incidentes de proteção de dados; política de segurança da informação; modelo de relatório de incidente de segurança de dados pessoais	Baixo
Roubo	princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD)	10	10	100	Médio	política de resposta de incidentes de proteção de dados; política de segurança da informação; modelo de relatório de incidente de segurança de dados pessoais	Baixo
Remoção não autorizada	princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD)	10	10	100	Médio	política de resposta de incidentes de proteção de dados; política de segurança da informação; modelo de relatório de incidente de segurança de dados pessoais	Baixo
Utilização de dados em excesso	princípio da necessidade (art. 6, II e III, LGPD)	10	10	100	Médio	Limitação da coleta/anonimização dos dados; governança de dados; segmentação dos dados; mapeamento de dados	Médio
Não especificação de quais as medidas de segurança adotadas	princípio da segurança (art. 6, VII e art. 46, LGPD)	5	15	75	Médio	Elevar os níveis de segurança, com política de segurança da informação implementada e atualizada; mapeamento de dados	Baixo

Execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.	princípio da qualidade dos dados (art. 6, V, LGPD)	5	15	75	Médio	mapeamento de dados realizado com precisão e qualidade (assegurar que os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento).	Baixo
Tratamento de dados pessoais de crianças e adolescentes sem o consentimento de pais ou responsáveis	princípio da segurança (art. 6, VII e art. 46) e princípio da responsabilização (art 6, X) e regras para tratamento de dados de crianças (art. 14, LGPD)	15	15	225	Alto	Anonimização dos dados; termos de uso; controle de acesso; política de segurança da informação; treinamento e orientação para os funcionários; coleta do consentimento dos pais e responsáveis; termo de consentimento	Médio
Retenção prolongada de dados pessoais sem necessidade.	Art. 5, inc. XIV, LGPD + Art. 18, IV e VI, LGPD	15	5	75	Médio	Controle do tempo de guarda [ciclo de vida]; controles de segurança em redes; política interna; governança de dados; mapeamento de dados pessoais	Baixo
O órgão/entidade não apresenta uma política de privacidade informando o tratamento realizado e dados pessoais tratados	Art. 50, § 3º, LGPD + Princípio da transparência	15	15	225	Alto	Elaborar política de segurança da informação, monitorar e auditar a privacidade; disponibilização no site do órgão	Baixo

Compartilhamento de dados excessivos com órgãos públicos	Art. 18, VII, LGPD + princípio da necessidade	10	5	50	Baixo	acordos de cooperação com entidades externas à Prefeitura para compartilhamento para fins de políticas públicas; informação de compartilhamento nos termos de uso; publicar no site do órgão a dispensa de consentimento; auditorias constantes para identificar novas necessidades de compartilhamento	Baixo
Informação insuficiente sobre a finalidade do tratamento	Art. 6º, I; art. 9º, I; art. 23, LGPD	10	15	150	Alto	Atualização dos termos de uso; atualização das políticas de compartilhamento; treinamento e orientação para os funcionários; atualização dos contratos, convênios, acordos de cooperação e instrumentos jurídicos congêneres; mapeamento de dados pessoais	Alto
Falha em considerar os direitos do titular dos dados pessoais (Ex.: não possibilitar remoção do consentimento)	Art. 9º; art. 18º, LGPD	10	10	100	Médio	Atualização dos termos de uso; modificação dos sistemas para permitir eliminação do dado, caso o titular revogue o consentimento; termos de uso; treinamento e orientação para os funcionários; termo de consentimento; plano de adequação à proteção de dados	Baixo

Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Art 5º, I; art. 13, §4º, LGPD	5	5	25	Baixo	identificar possibilidades de cruzamento de dados que estejam publicamente disponíveis de modo a permitir que a pessoa natural se torne identificada ou identificável	Baixo
Reidentificação de dados pseudonimizados	Art 5º, I; art. 13, §4º, LGPD	5	15	75	Médio	Utilizar tecnologias mais atualizadas para realizar a anonimização dos dados pessoais	Baixo

Referências:

Tabela 8. Matriz de Probabilidade X Impacto (CCGD, 2020).

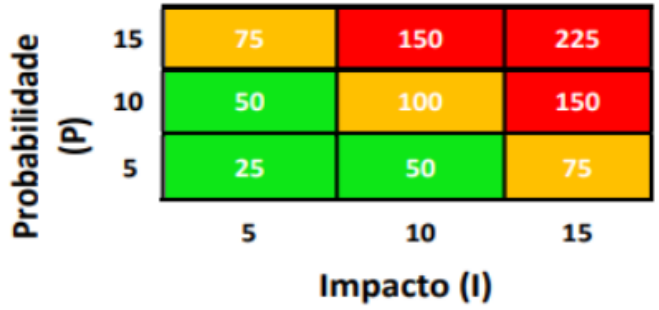

Tabela 9. Legenda de cores (CCGD, 2020).

Legenda (Cor)	Classificação do nível de risco
Verde	Baixo
Amarelo	Moderado
Vermelho	Alto

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P	I	NÍVEL DE RISCO (P X I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda	5	15	75
R04	Roubo	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

Legenda: P – Probabilidade; I – Impacto.