MATRIZ DE RISCOS LGPD - UNIDADE: SECRETARIA DE SAÚDE - DATA ATUALIZAÇÃO: 13/06/2023

IDENTIFICAÇÃO, AVALIAÇÃO E TRATAMENTO DE RISCOS
BASEADO NAS FICHAS DE TRATAMENTO DE DADOS PESSOAIS PREENCHIDAS PELAS UNIDADES DO TRT

RISCOS DE SISTEMAS E DE SEGURANÇA DA INFORMAÇÃO - PADRÃO PARA TODAS AS FICHAS DE TRATAMENTO DE DADOS

Valores comuns dos Riscos da LGPD antes das Medidas para o Tratamento dos Riscos.

SÃO 4 TIPOS DE TRATAMENTOS

ACEITAR	Risco é aceito (necessário justificar)
MITIGAR	Diminuir o Risco (probablidade de ocorrer)
EVITAR	Evitar o Risco (afeta o Impacto do risco)
TRANSFERIR	Transferir para Terceiros (Ex.: Seguradora)

RISCO	P	I	NÍVEL DE RISCO (P x I)	MEDIDAS ADOTADAS PARA O TRATAMENTO	EFEITO SOBRE O RISCO	OBSERVAÇÃO
R01 - Acesso não Autorizado	10	15	**150**	Controle de acesso do sistema (autenticação/ senha)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso
				Drive de rede com acesso restrito (autenticação / senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Armazenamento no Google Drive "nuvem" (autenticação/ senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
R02 - Modificação não autorizada	10	15	**150**	Controle de acesso do sistema (autenticação/ senha)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso
				Drive de rede com acesso restrito (autenticação / senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Armazenamento no Google Drive "nuvem" (autenticação/ senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
R03 - Perda	5	15	**75**	Controle de acesso do sistema (autenticação/ senha)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso
				Drive de rede com acesso restrito (autenticação / senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Armazenamento no Google Drive "nuvem" (autenticação/ senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Cópia de segurança (backup dos dados - Google / sistemas do TRT)	**MITIGAR**	Risco é mitigado com a utilização da política de cópia de segurança
				Histórico de acesso / alterações (google e/ou log do sistemas do TRT)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso/alterações
R04 - Roubo	5	15	**75**	Controle de acesso do sistema (autenticação/ senha)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso
				Drive de rede com acesso restrito (autenticação / senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Armazenamento no Google Drive "nuvem" (autenticação/ senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Cópia de segurança (backup dos dados - Google / sistemas do TRT)	**MITIGAR**	Risco é mitigado com a utilização da política de cópia de segurança
				Histórico de acesso / alterações (google e/ou log do sistemas do TRT)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso/alterações
R05 - Remoção não autorizada	5	15	**75**	Controle de acesso do sistema (autenticação/ senha)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso
				Drive de rede com acesso restrito (autenticação / senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Armazenamento no Google Drive "nuvem" (autenticação/ senha)	**EVITAR**	Risco é evitado, já que é necessário autorização para acessar
				Cópia de segurança (backup dos dados - Google / sistemas do TRT)	**MITIGAR**	Risco é mitigado com a utilização da política de cópia de segurança
				Histórico de acesso / alterações (google e/ou log do sistemas do TRT)	**MITIGAR**	Risco é mitigado com a utilização do controle de acesso/alterações

RISCOS DE PRIVACIDADE DOS DADOS PESSOAIS
ESPECIFÍCO PARA A FICHA: GESTÃO DE SAÚDE DE MAGISTRADOS E SERVIDORES

RISCO	P	I	NÍVEL DE RISCO (P x I)	MEDIDAS ADOTADAS PARA O TRATAMENTO	EFEITO SOBRE O RISCO	OBSERVAÇÃO
R06 - Coleção excessiva (Coleta de dados pessoais em quantidade superior ao necessário)	10	10	**100**	Por se tratar de dados de gestão de saúde de magistrados e servidores, é necessário uma coleta de dados maior e muito mais completa de dados pessoas, incluindo dados pessoais sensíveis.	**MITIGAR**	Como são dados pessoas e também dados sobre a saúde de magistrados e servidores, é necessário uma coleta maior de dados. Por se tratar de informações médicas, por lei, os dados são protegidos por sigilo médico, além de outras medidas de proteção para garantir a confidencialidade das informações.
R07 - Informação insuficiente sobre a finalidade do tratamento de dados	10	15	**150**	Conforme ficha de tratamento de dados pessoas, a finalidade consta nos sistemas e prontuários médicos que são preenchidos com dados pessoais fornecidos pelo próprio titular e a finalidade também é a de preservar o sigilo médico dos dados pessoais sensíveis.	**EVITAR**	A finalidade do tratamento de dados consta nos sistemas e formulários que são preenchidos pelo próprio titular dos dados pessoais.
R08 - Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	10	15	**150**	Os titulares de dados pessoais fornecem os dados pessoais via sistemas (proad, sigs de saúde) e formulários de saúde.	**EVITAR**	Risco está sendo evitado, já que o titular dos dados pessoais está fornecendo os dados. Também conforme a Lei 13,709/ 2018, art. 7º, III, a Administração Pública pode efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas para entrega de serviços públicos
R10 - Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	**150**	Os dados são compartilhados internamente ou com outros órgãos públicos que solicitem avalição médicas de seus servidores	**EVITAR**	Os dados são compartilhados interna e externamente dentro da administração pública.
R11 - Retenção prolongada de dados pessoais sem necessidade.	10	5	**50**	Na Ficha de Tratamento de dados consta o prazo como: **a definir** Será necessário verificar se existe prazo legal ou se pode colocado algum prazo para retenção.	**ACEITAR**	**Neste caso, como o Risco consta como baixo na tabela (cor verde) não é necessário medidas para o tratamento do risco (seria opcional) e portanto o Risco pode ser considerado Aceito.**