

	Política de Avaliação de Risco de Segurança e Privacidade	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 1 / 16

Considerações Iniciais

A Lei Geral de Proteção de Dados Pessoais – LGPD, em seu capítulo VII, Seção I, Art. 46, dispõe: *“Os agentes de tratamento devem adotar 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”.*

Diante disto, a melhor maneira de determinar onde e como deve-se intensificar os esforços para proteção das informações é realização a Avaliação/ Gestão de Riscos.

Uma avaliação de riscos realizada de forma correta, com uma metodologia adequada (conforme prega a ISO 31000 – Gestão de Riscos), pode dizer onde estão os principais riscos e impactos, e conseqüentemente nos mostrando onde devemos colocar nossos esforços num primeiro momento.

Especificamente a matriz de riscos ou matriz de probabilidade e impacto é uma ferramenta de gerenciamento de riscos que permite de forma visual identificar quais são os riscos que devem receber mais atenção.

A avaliação de riscos também permitirá identificar, analisar e avaliar as ameaças e vulnerabilidades que expõem os dados pessoais que estão sendo tratados.

Sumário

1. Objetivo	2
2. Abrangência	2
3. Definições	2
4. Diretrizes	3
5. Benefícios da Avaliação de Riscos	4
6. Etapas de Elaboração	4
7. Categorias de Riscos	6
8. Análise dos Riscos	7
9. Exemplos de Riscos identificados quanto ao tratamento de dados pessoais	9
10. Tratamento dos riscos identificados	11
11. Monitoramento e análise crítica	12
12. Comunicação e Consulta dos Riscos	13
13. Responsabilidades	13
14. Sanções	15
15. Anexos	15
16. Referências	16
17. Disposições Finais.....	16
18. Histórico de revisões	16

	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 2 / 16

1. Objetivo

Essa política tem por fim definir e implementar estratégia para atuar preventivamente nas frentes de segurança da informação e privacidade de dados, com o intuito de fomentar a cultura de proteção de dados, implementando ações que visam avançar no processo de adequação à LGPD, minimizando os riscos durante todo o tratamento de dados pessoais, desde a fase de concepção até o seu correto descarte (Privacy by Design and Default).

2. Abrangência

Esta Política estabelece as diretrizes a serem observadas por todos os colaboradores, independentemente das atividades que desempenham, cargo ou função que ocupam e unidade em que estejam alocados, bem como por todos os clientes, usuários, fornecedores, prestadores de serviços, parceiros que venha a se relacionar com o Grupo Patense.

3. Definições

3.1. Risco: Possibilidade de evento que afeta negativamente a realização dos objetivos da Empresa ou de seus processos.

3.2 Análise de risco: Uso sistemático de informações para identificar fontes e estimar o risco

3.3. Identificação de riscos: Processo para localizar, listar e caracterizar elementos do risco.

3.4. Gestão de riscos: Atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco.

3.5. Apetite ao risco: Grau de exposição aos riscos que o Grupo Patense está disposto a aceitar para atingir seus objetivos estratégicos.

3.5. Informação: Conhecimento apresentado a uma pessoa em uma forma que possa ser compreendida. Dados que foram processados ou organizados para que tenham significado. A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida.

	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 3 / 16

3.6. Segurança da Informação: Preservação da confidencialidade, integridade e disponibilidade da informação.

4. Diretrizes

4.1. Garantir a segurança da informação e privacidade, e padronizar as práticas a serem aplicadas por todo o pessoal com responsabilidade para a segurança da informação e privacidade.

4.2. Dar consciência dos riscos que ameaçam o sistema de informação e os meios disponíveis para controlá-los.

4.3. Criar uma estrutura geral para projetar e executar medidas de segurança dos sistemas de informação; e

4.4. Promover a cooperação entre os departamentos do Grupo Patense para criar, aplicar e verificar as instruções, procedimentos e medidas de segurança relacionadas ao negócio.

4.5. Ainda são diretrizes desta política aquelas que definem e caracterizam as etapas macro do processo de Gestão de Riscos de Segurança da Informação e Privacidade do Grupo Patense:

4.5.1. Identificação dos Riscos: A identificação de riscos tem o objetivo de reconhecer e descrever os riscos aos quais a Empresa está exposta.

4.5.2. Avaliação dos Riscos: Após a identificação dos riscos, são realizadas análises qualitativas e quantitativas, visando a definição dos atributos de impacto e probabilidade, utilizados na priorização dos riscos a serem tratados.

4.5.3. Estratégia dos riscos: Após a avaliação dos riscos, são realizadas estratégias de tratamento dos riscos, visando a definição dos itens abaixo:

- Reduzir
- Aceitar
- Transferir
- Evitar

❖ Esta etapa inclui o grau de importância na implementação de um controle sobre o risco, bem como, o levantamento e a análise dos controles já existentes.

4.5.4 Tratamento dos Riscos: Posteriormente à etapa de validação dos controles, é definido o tratamento que será dado aos riscos e como estes devem ser monitorados e comunicados às diversas partes envolvidas.

4.5.5. Monitoramento dos Riscos: Visando o aprimoramento contínuo da Gestão de Riscos, o processo de monitoramento consiste em acompanhar o desempenho dos indicadores de riscos, supervisionar a implantação e manutenção dos planos de ação e o alcance das metas estabelecidas, através de atividades gerenciais contínuas e/ou avaliações independentes.

4.5.6. Comunicação dos Riscos: A comunicação durante todas as etapas do processo de gestão integrada de riscos atinge a todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas pelo mercado.

5. Benefícios da Avaliação de Riscos



6. Etapas de Elaboração

6.1. Data Mapping

É fundamental que a avaliação de riscos seja realizada apenas depois que os processos e setores foram mapeados através do Data Mapping (mapeamento de dados), onde é possível identificar as características do processo em relação aos dados pessoais envolvidos (quais dados estão sendo tratados, fluxo de vida dos dados, responsáveis, armazenamento, destino, descarte).

	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 5 / 16

O Data Mapping também pode ser conhecido como inventário de dados, e tem como principal objetivo analisar todo o caminho que o dado pessoal percorre desde o momento em que é coletado pela organização até o seu descarte.

Somente assim será possível analisar os principais riscos que envolvem as atividades realizadas por cada setor do GRUPO PATENSE. Cada processo que envolva dados pessoais, deve ser avaliado de forma individualizada, mesmo que alguns riscos sejam inerentes a vários outros processos.

6.2. Relatório de Impacto à Proteção de Dados Pessoais

O primeiro passo a ser dado é tentar identificar as fases do processo de gestão de riscos, especificamente no que se refere proteção de dados pessoais e dados pessoais sensíveis. Em razão disso a LGPD trouxe alguns conceitos relacionado a avaliação de riscos, vejamos:

“Art. 5º, XVII – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

Este relatório também chamado de DPIA ou RIPD, consiste na análise dos impactos dos dados pessoais. Para elaboração do DPIA é preciso **realizar a avaliação de riscos dos processos que envolvem dados pessoais**. Também no Art. 50, § 1º a LGPD estabelece que *“Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a **probabilidade e a gravidade** dos riscos e dos benefícios decorrentes de tratamento de dados do titular”.*

Com a realização da avaliação de riscos, a empresa pode garantir que sejam implementados níveis apropriados de medidas técnicas e organizacionais para proteção dos dados pessoais e evitar que riscos ocorram.



	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 6 / 16

6.3. Processos e Pessoas

A avaliação de riscos não deve ser focada apenas em tecnologia, mas também em processos e pessoas, diante disto para identificação dos riscos, é necessário definir responsáveis e realizar a coleta dos dados.

6.3.1. Definir Responsáveis

A definição dos responsáveis consiste na identificação do responsável pelo tratamento do risco. Dessa forma, cada atividade, que apresenta probabilidade de risco ao tratamento de dados, deve ter esta pessoa envolvida, que no GRUPO PATENSE, é a Encarregada de Proteção de Dados Pessoais com o apoio do setor de TI.

6.3.2. Realizar Coleta de Dados

Após a definição da Encarregada de Proteção de Dados como responsável de analisar o risco de cada projeto, e diante das informações obtidas através do mapeamento de dados, será realizada a coleta de informações para definição da lista de riscos.

- **Brainstorming:** Identificar os riscos e suas fontes em reuniões com equipe multidisciplinar de especialistas, contando com a orientação de um facilitador.
- **Entrevistas:** Identificar os riscos em reuniões com partes interessadas, especialistas ou pessoas com experiência no processo. Garantir um ambiente de confiança e confidencialidade para coleta de informações mais precisas.

7. Categorias de Riscos

Abaixo será apresentada uma lista não taxativa das categorias de alguns riscos que poderão ser identificados:

- Acesso não autorizado;
- Modificação não autorizada;
- Perda;
- Roubo;

	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 7 / 16

- Remoção não autorizada;
- Coleta excessiva;
- Informações insuficientes sobre a finalidade do tratamento;
- Tratamento sem consentimento do titular dos dados pessoais;
- Falha em considerar os direitos do titular dos dados pessoais;
- Compartilhar ou distribuir dados pessoais com terceiros;
- Retenção prolongada de dados pessoais sem necessidade;
- Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular;
- Falha ou erro de processamento;
- Reidentificação de dados pseudonimizados.

8. Análise dos Riscos

A análise dos riscos consiste em aprofundar o nível de compreensão em relação à natureza dos riscos, bem como o nível do impacto nos objetivos de cada projeto, processos e ou atividades. E isso é feito através da avaliação de probabilidade x impacto e elaboração da respectiva matriz de risco.

Probabilidade

- Sem Risco: Não existem informações que indiquem a ocorrência;
- Baixo Risco: Existem poucos indícios que indiquem a ocorrência;
- Alto Risco: Existem registros históricos de grande repetição ou indício forte que apontam para a possibilidade de ocorrência;
- Risco Máximo: As evidências apontam para a garantia quase certa de ocorrência.

Impacto

- Insignificante: Impacto mínimo no processo;
- Limitado: Impacto discreto sem representar ameaça aos objetivos;
- Significante: Impacto direto nos objetivos com grande dificuldade de recuperação;
- Máximo: Impacto grave que inviabiliza a possibilidade de recuperação.

A Matriz de Risco será elaborada com base nas informações coletadas no Data Mapping bem como após a avaliação de probabilidade e impacto destas atividades.

	Política de Avaliação de Risco de Segurança e Privacidade	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 8 / 16

Risco Máximo	10	40	80	100
Alto Risco	8	35	64	80
Baixo Risco	4	16	32	40
Sem Risco	1	4	8	10
	Insignificante	Limitado	Significante	Máximo

Cada risco deve ser classificado entre RB (Risco Baixo), RM (Risco Médio) e RA (Risco Alto), dessa forma as ações serão planejadas com base no nível de criticidade identificado:

- **RB (Risco Baixo):** Aceitar riscos e manter ações de monitoramento;
- **RM (Risco Médio):** Gerenciar riscos e manter monitoramento das ações de tratamento;
- **RA (Risco Alto):** Exige grande esforço para gerenciamento dos riscos e acompanhamento extensivo das ações de tratamento. Considere a execução constante do processo “4. Monitoramento e Análise Crítica”.
- **RM (Risco Máximo):** Exige que o projeto seja reelaborado ou caso não seja possível essa reanálise que não seja dado prosseguimento em razão do alto risco de incidente de segurança da informação e/ou vazamento de dados pessoais.

Mais informações sobre PROBABILIDADE e IMPACTO:

Probabilidade		Descrição dos critérios de probabilidade
Numérica	Descritiva	
1% a 10%	Muito baixa	Não é provável que aconteça
11% a 30%	Baixa	Pode ser que ocorra uma vez dentro de um ano
31% a 50%	Moderada	Pode ser que ocorra mais de uma vez dentro de um ano
51% a 70%	Alta	Pode ser que ocorra mensalmente
71% a 90%	Muito alta	Pode ser que ocorra semanalmente

Impacto	Descrição
Muito baixo	Os riscos possuem consequências pouco significativas
Baixo	Os riscos possuem consequências reversíveis em curto e médio prazo com custos pouco significativos
Moderado	Os riscos possuem consequências reversíveis em curto e médio prazo com custos baixos
Alto	Os riscos possuem consequências reversíveis em curto e médio prazo com custos altos
Muito alto	Os riscos possuem consequências irreversíveis ou com custos inviáveis

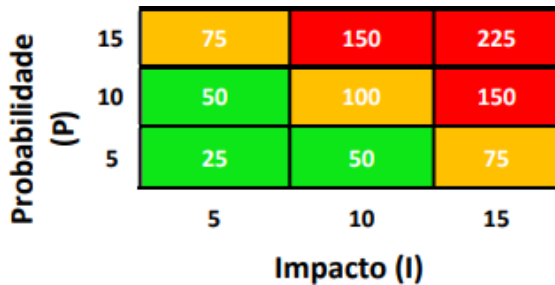


Tabela 9. Legenda de cores (CCGD, 2020).

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

Tabela. Matriz de Probabilidade X Impacto (CCGD, 2020), do Guia de avaliação de Riscos de Segurança e Privacidade

O conhecimento sobre o risco identificado é fundamental para que a avaliação seja realista e precisa. Além disso, a avaliação do risco pode ser feita por um time ao invés de apenas por uma pessoa. As discussões geradas ajudarão a entender e esclarecer qual é o nível real de impacto e probabilidade do risco sob avaliação.

Uma dica para estimular a reflexão nesse momento é fazer perguntas como: “O quanto sabemos sobre esse risco? Já lidamos com ele antes? Temos algum fato ou dado sobre o risco (por exemplo, incidências, indicadores...)?”. Essas perguntas não ajudarão somente a avaliação de impacto e probabilidade, mas também na definição de ações de tratativa do risco.

Ao determinar a probabilidade e impacto do risco, esses valores devem ser inseridos na linha e coluna correspondente ao resultado obtido, gerando assim a classificação do risco. De acordo com a classificação do risco será possível **definir se ele deve ser tratado ou não como prioridade**.

9. Exemplos de Riscos Identificados quanto ao Tratamento de Dados Pessoais

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.

Tabela. Riscos e níveis de riscos referente ao tratamento de dados pessoais (CCGD, 2020), do Guia de Avaliação de Riscos de Segurança e Privacidade.

	Política de Avaliação de Risco de Segurança e Privacidade	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 11 / 16

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO	RISCO RESIDUAL			MEDIDA(S) APROVADA(S)
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso Lógico.	Reduzir	5	10	50	Sim
	2. Desenvolvimento seguro.					
	3. Segurança em Redes.					

Legenda: P – Probabilidade; I – Impacto.

Tabela. Exemplos de medidas para lidar com os riscos (CCGD, 2020), do Guia de Avaliação de Riscos de Segurança e Privacidade.

10. Tratamento dos Riscos Identificados

O tratamento dos riscos é uma atividade para identificação e definição de estratégias e planejamento de ações para lidar com a exposição aos riscos.

As ações definidas devem visar o objetivo principal dos processos dentro do contexto da LGPD, buscando a conformidade com a legislação vigente.

As ações planejadas devem ser realistas em relação à disponibilidade de recursos humanos, financeiros e de prazo. O responsável pelo processo deve garantir a qualidade das ações definidas, realizando o acompanhamento e as alterações necessárias, sempre que identificadas.

A descrição de cada ação deve ser norteada por uma das 4 categorias, descritas a seguir:

- **Prevenir:** Alterar o processo, deixando de executar a atividade que representa o risco identificado;
- **Transferir/Compartilhar:** Transferir parcialmente ou integralmente o risco para terceiros;
- **Mitigar/Melhorar:** Reduzir o impacto e/ou a probabilidade de ocorrência do risco para níveis aceitáveis;
- **Aceitar:** Definir se a aceitação do risco será de forma passiva, não sendo necessária nenhuma ação, ou ativa, definindo reservas de contingência financeiras, de prazo ou de recursos humanos.

O conjunto de informações definidas nos processos 1. Identificação dos Riscos, 2. Análise dos Riscos e Tratamento dos riscos resultam no plano para tratamento dos riscos, com o propósito de especificar “como

	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 12 / 16

as opções de tratamento escolhidas serão implementadas, de maneira que os arranjos sejam compreendidos pelos envolvidos e o progresso em relação ao plano possa ser monitorado” (ABNT, 2018).

Poderão também ser implementados controles de riscos. À medida que os controles são implementados, a classificação da probabilidade ou do impacto é reduzida, vejamos:

Controles implementados	Probabilidade	Impacto
0 a 50 por cento	Alta	
50 a 85 por cento	Moderada	Alto
85 a 100 por cento	Baixa	Moderado

Tabela. Controles implementados X classificação do Guia de Avaliação de Riscos de Segurança e Privacidade

11. Monitoramento e Análise Crítica

O Monitoramento e Análise Crítica tem como objetivo garantir o bom andamento dos planos definidos. Nesta etapa, os responsáveis devem “assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo” (ABNT, 2018).

É necessário reavaliar riscos, realizar auditorias, realizar análise crítica, medir os desempenhos.

11.1. Reavaliar Riscos

Revisar os riscos mapeados para atualizar as informações com novos riscos identificados, atualização de riscos já descritos e exclusão de riscos desatualizados.

11.2. Realizar Auditoria

Examinar o desempenho do processo de gestão de riscos e das ações adotadas para tratamento dos riscos identificados.

11.3. Realizar Análise Crítica

Realizar a análise dos riscos e de seus tratamentos. O setor envolvido, nos diferentes níveis de gestão, deve realizar autoavaliação, na busca contínua por melhorias dos processos de trabalho e nos dados cadastrados.

	Política de Avaliação de Risco de Segurança e Privacidade	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 13 / 16

11.4. Medir Desempenho

Comparar o desempenho técnico do andamento das ações definidas frente ao planejamento realizadas nas etapas anteriores.

12. Comunicação e Consulta dos Riscos

O processo de comunicação e consulta é executado de forma permanente com ações, partindo da divulgação dos planos para gestão dos riscos até o final dos tratamentos identificados e executados, para cada risco dos processos. “A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação, para auxiliar a tomada de decisão”(ABNT, 2018).

É necessário realizar dentro da empresa ampla divulgação da necessidade de análise de riscos em cada novo projeto a ser executado, bem como é necessário facilitar a comunicação para coletar informações sobre a eficiência do plano de gestão de riscos na perspectiva do setor interessado.

A transparência, confidencialidade e a garantia de privacidade dos colaboradores devem ser princípios fundamentais para a execução dessa atividade.

13. Responsabilidades

13.1. Área de Gestão de Risco (Setor de TI e Encarregado de Proteção de Dados)

- Garantir o atendimento desta política;
- Acompanhar a gestão de riscos, validando e revisando periodicamente a matriz de riscos do Grupo Patense, assim como a estrutura de controles internos capazes de minimizar a ocorrência de riscos;
- Definir os riscos a serem priorizados para tratamento, com base no grau de exposição ao risco;
- Avaliar o desempenho dos indicadores de riscos, de modo a alinhá-los aos objetivos estratégicos do Grupo;
- Prover o alinhamento de assuntos estratégicos e operacionais no processo de gestão integrada de riscos;
- Revisar e avaliar a eficácia dos processos de trabalho da gestão integrada de riscos;

	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 14 / 16

- Reportar à Diretoria os resultados do processo de gerenciamento dos riscos;
- Revisar a presente política sempre que necessário;
- Indicar os proprietários de riscos;
- Homologar os planos de ação para mitigação dos riscos das áreas do Grupo;
- Disseminar a cultura de gerenciamento de riscos, conscientizando os colaboradores sobre os riscos inerentes ao negócio e suas responsabilidades no processo de gestão integrada de riscos;
- Avaliar, monitorar e propor procedimentos que mitiguem os riscos de violação dos dados pessoais por ela coletados, armazenados e descartados.
- Prover recursos para a gestão, operação e monitoramento adequado das atividades de Segurança e Privacidade das Informações;
- Garantir a contínua análise e realimentação dos resultados de gestão de riscos;
- Propor os recursos necessários às ações de segurança da informação e comunicações;
- Revisar periodicamente o nível de segurança de sistemas internos;
- Manter-se atualizado com relação à tecnologia, legislação e novas ameaças;
- Analisar criticamente os incidentes de segurança mais significativos e gerenciar e/ou acompanhar as ações relacionadas na solução dos mesmos;
- Acompanhar o sistema de ações corretivas e preventivas relacionados à Privacidade e Segurança das Informações;
- Definir procedimentos que estejam alinhados aos princípios e diretrizes de Segurança da Informação.

13.2. Colaboradores

- Conhecer e seguir os procedimentos constantes nesta Política;
- Identificar qualquer incidente de segurança e reportá-lo ao seu gestor/contato direto dentro do Grupo Patense, e
- Cuidar pela proteção dos ativos de informação a que tiverem acesso.
- Assegurar medidas básicas de segurança para evitar situações de riscos

13.3. Encarregado de Proteção de Dados

- Aprovar a presente Política, e futuras revisões
- Definir e desenvolver as estratégias de Segurança da Informação e Privacidade em alinhamento com o Plano Estratégico do Grupo Patense;

	<h2>Política de Avaliação de Risco de Segurança e Privacidade</h2>	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 15 / 16

- Acompanhar as ações do Setor de Tecnologia da Informação relacionadas à Segurança da Informação e Privacidade.
- Aprovar o grau de apetite a riscos do Grupo Patense e as faixas de tolerância a desvios em relação aos níveis aceitáveis de riscos

13.4. Gestores

- Gerenciar os riscos inerentes aos processos de negócio que lhes cabem;
- Otimizar as decisões baseadas nos riscos;
- Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto a proteção da Segurança da Informação em sua área de atuação;
- Informar/comunicar todos os fatos relacionados à Gestão de Privacidade e Segurança da Informação às áreas de operação sob sua responsabilidade;
- Implantar as oportunidades de melhoria;
- Planejar a adoção de procedimentos relacionados à Gestão de Privacidade e Segurança da Informação e monitorar sua eficácia em sua área de atuação; e
- Garantir a contínua eficácia dos controles implantados para satisfazer os requisitos relacionados à Gestão de Privacidade e Segurança da Informação.

14. Sanções

14.1. O colaborador que descumprir quaisquer das disposições previstas nesta Política, no Código de Ética e Conduta e todas as demais Políticas relacionadas à sua atuação na Companhia bem como à legislação correspondente, estará expondo todo o Grupo à penalidades, e portanto, estará sujeito também a eventuais implicações judiciais ou administrativas decorrentes do descumprimento legal e aplicação de medidas disciplinares de acordo com a análise do caso concreto.

14.2. Os agentes de tratamento de dados (Controlador e/ou Operador), em razão das infrações cometidas às normas previstas na LGPD, ficam sujeitos às sanções administrativas aplicáveis pela autoridade nacional previstas no artigo 52 da referida legislação.

15. Anexos

- Anexo I – Avaliação de Riscos de Segurança e Privacidade

	Política de Avaliação de Risco de Segurança e Privacidade	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 16 / 16

16. Referências

- Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais

17. Disposições finais

17.1. Esta política está alinhada às demais políticas das empresas do Grupo Patense.

17.2. Esta política pode ser desdobrada em outros documentos normativos específicos, sempre alinhados aos princípios e diretrizes aqui estabelecidos.

17.3. Esta política deverá seguir e respeitar todas as diretrizes da Lei Geral de Proteção de Dados – Lei nº 13.709/2018, se aplicável, e as normas internas a ela vinculada.

17.4. Esta política deve ser revisada sempre que necessário e mediante a realidade do Grupo Patense.

17.5. É de responsabilidade do setor de Pessoas e Performance juntamente com o Setor de TI, garantir que esta política seja de conhecimento de todos os colaboradores das áreas envolvidas, através de treinamentos e informes, utilizando-se as ferramentas de comunicação que forem necessárias.

18. Histórico de Revisões

Data	Nº Versão	Item revisado	Descrição da revisão
08/09/2022	00		Elaboração da política
13/12/2023	01	Geral	Colocação no modelo padrão de governança
11/02/2025	02	Geral	Atualização de informações
29/01/2026	03	Geral	Revisão Anual
Emissor	Nome Denise R. Vilaça		Função Encarregada de Proteção de Dados
Revisor	Nome		Função
	Poliana C Gonçalves		Assistente de Governança Corporativa

	Política de Avaliação de Risco de Segurança e Privacidade	Nº DOCUMENTO CORP.TI.POL.003
		DATA DE EMISSÃO 08/09/2022
		VERSÃO 03
		PÁGINA 17 / 16

11/02/2024	Aline Pelet	Governance Officer
29/01/2026	Denise R Vilaça	Gerente Adm e Compliance Corporativo
Aprovador	Nome	Função
	Denise R. Vilaça	Gerente Adm e Compliance Corporativo

Presidente Grupo Patense