

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 1 / 17

Considerações Iniciais

A Política de Gestão de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação relacionados ao Grupo Patense e visa orientar o funcionamento do processo de gestão de incidentes de segurança da informação, de forma que estes sejam tratados adequadamente reduzindo ao máximo os impactos para o negócio.

Sumário

1. Objetivo	2
2. Abrangência.....	2
3. Definições	2
4. Diretrizes	4
5. Dos Critérios Gerais sobre os Incidentes de Segurança da Informação.....	4
6. O que fazer em caso de Incidente de Segurança com Dados Pessoais?.....	7
7. O que comunicar à Autoridade Nacional de Proteção de Dados	8
8. Dos Procedimentos a serem adotados.....	9
9. Em que situação e o que comunicar ao titular dos Dados	12
10. Qual o prazo para comunicar um Incidente de Segurança para a Autoridade Nacional de Proteção de Dados.....	13
11. Responsabilidades.....	13
12. Sanções	15
13. Anexos	15
14. Referências.....	15
15. Disposições Finais	16
16. Histórico de revisões	16

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 2 / 17

1. Objetivo

Estabelecer diretrizes para o gerenciamento de resposta a incidentes de segurança documentada e formalizada, onde a conformidade com a política e com os procedimentos de suporte colaboram para garantir a segurança dos recursos de sistema da Empresa.

2. Abrangência

Esta política tem abrangência corporativa em todas as unidades do Grupo Patense, ou seja, afeta todas as suas áreas de negócio, filiais, escritórios e demais operações no que se refere a ocorrência de incidentes de segurança da informação.

3. Definições

3.1. Informação: Qualquer conjunto de dados que resulte em algum significado compreensível. A informação pode possuir algum valor para o Grupo Patense, seus clientes, parceiros e colaboradores, bem como pode ser de propriedade da empresa ou estar sob sua custódia.

3.2. Segurança da informação: está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade (CID):

- a) Confidencialidade:** refere-se a restrição de acesso a informação apenas a pessoas autorizadas.
- b) Integridade:** se consubstancia na garantia da informação não ser perdida ou manipulada indevidamente.
- c) Disponibilidade:** é a garantia que a informação esteja disponível para uso legítimo por pessoa autorizada.

3.3. Colaborador: entende-se como colaborador qualquer pessoa que trabalhe para o Grupo Patense, quer seja funcionário com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee.

3.4. Gestor: colaborador que exerce cargo de liderança, como presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção.

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 3 / 17

3.5. Recurso: qualquer ativo, tangível ou intangível, pertencente a serviço ou sob responsabilidade do Grupo Patense, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

3.6. Incidentes de Segurança: violação da segurança dos sistemas, arquivos, bases, equipamentos e/ou locais utilizados pela Operadora que leve à destruição, perda, alteração, acesso, aquisição, divulgação, utilização ou acesso ilegal a dados pessoais associados à Controladora de algum modo tratados pela Operadora.

3.7. Dado pessoal: todos e quaisquer dados ou informações que, individualmente ou em conjunto com outros dados ou nomes, identifiquem ou permitam que um determinado Titular de Dados seja identificado, incluindo: (i) dados que forem definidos explicitamente como uma categoria de dados pessoais, nos termos da Lei 13.709/2018 (“LGPD”); (ii) dados pessoais não públicos, tais como o número de identidade (RG), número de passaporte, número de seguro social (ou número equivalente), número de licença do motorista, CPF, endereço, telefone, e-mail, contato em redes sociais, nome dos pais de uma pessoa, data de nascimento, número do título de eleitor, entre outros, e/ou (iii) informações financeiras, tais como número de conta bancária, entre outras relacionadas.

3.8. Dados pessoais sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

3.9. Tratamento: qualquer operação realizada com dados pessoais, por meio analógico ou digital, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, extração, comparação, interconexão ou destruição.

3.10. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

3.11. Controladora: pessoa a quem compete as decisões referentes ao tratamento de dados pessoais.

(Exemplo: A Patense trata os dados pessoais de seus colaboradores em razão do seu contrato de trabalho e dos seus fornecedores/ clientes em razão da relação comercial.)

3.12. Operadora: pessoa que realiza o tratamento de dados pessoais em nome do controlador. O operador somente poderá processar dados pessoais de acordo com as instruções fornecidas pelo controlador, ou seja, o controlador é quem estabelece as finalidades e limites do tratamento de dados.

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 4 / 17

(**Exemplo:** funcionários terceiros ingressão dentro das suas dependências para prestar algum serviço e necessitamos analisar os documentos como ficha de EPI e certificados de treinamentos. A empresa contratada e responsáveis por estes colaboradores é a Controladora de seus dados e a Patense é operadora).

3.13. ANPD: Autoridade Nacional de Proteção de Dados. Órgão da administração pública federal, integrante da Presidência da República que possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a fiscalização do cumprimento da Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados – LGPD.

3.14. Encarregado de Proteção de Dados: responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD.

4. Diretrizes

4.1. Devem ser implementados sistemas de salvaguarda e mecanismos de controle para proteção dos recursos de sistema em todo o Grupo Patense, reforçando os sistemas críticos quanto à segurança da informação.

4.2. Os usuários autorizados devem adotar as devidas diligências para detectar um incidente ou anormalidades no sistema.

4.3. O plano de de ação e resposta a incidentes, estabelecido pelo Grupo Patense, deve ser seguido para minimizar o impacto do incidente na infraestrutura crítica de rede e sistema do Grupo.

4.4. Uma vez que o sistema afetado é restabelecido, deve ser realizada uma análise técnica para examinar detalhadamente a integridade dos dados.

4.5. Deve ser atribuído o nível de impacto causado pelo incidente de acordo com parâmetros definidos nesta política, conforme item 5.16.

5. Dos Critérios Gerais sobre os incidentes de Segurança da Informação

5.1. São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 5 / 17

um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco.

5.2. O art. 47 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) determina que os agentes de tratamento de dados pessoais 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.

5.3. Todos os colaboradores devem estar em capacidade de identificar incidentes de segurança da informação quando for testemunhado.

5.4. Todos os colaboradores devem notificar imediatamente a Controladora, por meio do Setor de Tecnologia da Informação e o Encarregado de Proteção de Dados qualquer evento de segurança ou fragilidade observada que possam causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas da empresa

5.5. Vulnerabilidades ou fragilidades suspeitas também devem ser imediatamente comunicadas e não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança cibernética e da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

5.6. A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política.

5.7. Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

5.8. Indisponibilidade do ambiente tecnológico em virtude de ataque maliciosos interno e externo;

5.9. Vazamento de informações confidenciais (informações de clientes, informações estratégicas, outros) através de e-mails encaminhados de forma equivocada a destinatários que não tem relação com o assunto ou por de aplicativos eletrônicos, como WhatsApp;

5.10. Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente de TI;

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 6 / 17

5.11. Ato de violar uma política de segurança, explícita ou implícita; VI. Uso ou acesso não autorizado a um sistema;

5.12. Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema.

5.13. Compartilhamento de senhas com usuários não autorizados.

5.14. Violações ou tentativas de violação da Diretriz de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

5.15. **Deixar documentos a vista em cima da mesa, não bloquear a tela do computador ao sair da sala, deixar documentos com informações importantes próximos às impressoras.**

5.16. Serão utilizadas escalas quantitativas para estimar a probabilidade e o impacto dos riscos de incidentes de segurança da informação:

Peso	Critérios	Probabilidade
5	Muito Alta	50% < Probabilidade <= 100%
4	Alta	20% < Probabilidade <= 50%
3	Média	8% < Probabilidade <= 20%
2	Baixa	2% < Probabilidade <= 8%
1	Muito Baixa	0% < Probabilidade <= 2%

Peso	Impacto	Descrição
5	Catastrófico	Impacto máximo nos objetivos do processo avaliado, sem possibilidade de recuperação.
4	Muito Relevante	Impacto significativo nos objetivos do processo avaliado, com possibilidade remota de recuperação.
3	Relevante	Impacto mediano nos objetivos do processo avaliado, com possibilidade de recuperação.
2	Pouco Relevante	Impacto mínimo aos objetivos do processo avaliado. São facilmente remediáveis.
1	Insignificante	Impacto insignificante nos objetivos do processo avaliado. Dispensa qualquer medida de reparação.

- O nível de risco é calculado pelo produto entre a probabilidade e o impacto. A tabela abaixo representa a matriz de risco, ferramenta utilizada para a classificação dos níveis de risco:

		PROBABILIDADE				
		Muito baixa (1)	Baixa (2)	Média (3)	Alta (4)	Muito Alta (5)
IMPACTO	Catastrófico (5)	5	10	15	20	25
	Muito relevante (4)	4	8	12	16	20
	Relevante (3)	3	6	9	12	15
	Pouco Relevante (2)	2	4	6	8	10
	Insignificante (1)	1	2	3	4	5
		Baixo				
	Médio					
	Elevado					
	Extremo					

6. O que fazer em caso de incidente de segurança com dados pessoais?

6.1. Avaliar internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis. Vide formulário de avaliação constante do sítio eletrônico da ANPD;

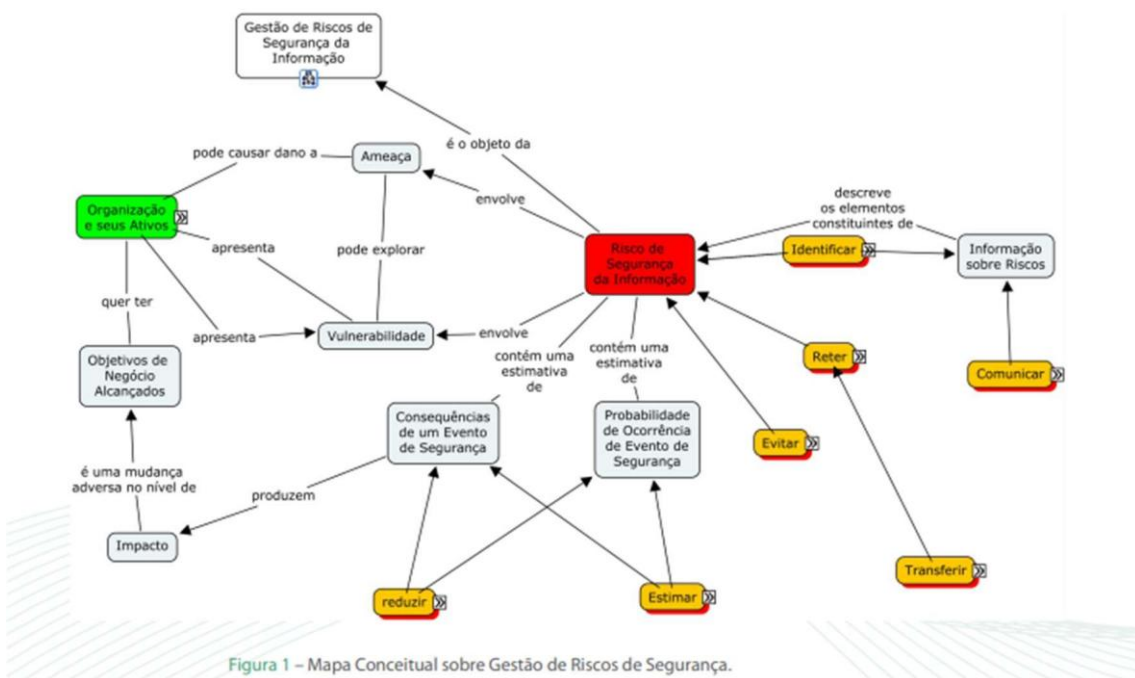
6.2. Comunicar a Controladora através do Setor de Tecnologia da Informação e do Encarregado de Proteção de Dados (Art. 5º, VIII da LGPD);

6.3. O conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida.;

6.4. Comunicar a Controladora, se você for o operador, nos termos da LGPD;

6.4.1. Comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD); e;

6.4.2. Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).



7. O que comunicar à Autoridade Nacional de Proteção de Dados?

7.1. O Encarregado pela Proteção de Dados da Patense será o canal de comunicação com a ANPD e demais participantes para notificar qualquer incidente relacionado à privacidade de dados:

Encarregado pela Proteção de Dados da Patense
Denise Vilaça
e-mail: lgpd@patense.com.br
Telefone: (34) 3818.1847
Endereço: Rua Doutor Marcolino, nº 79, Centro, Patos de Minas – MG

7.2. As informações devem ser claras e concisas. Além do que prescreve o § 1º do artigo 48 da LGPD, recomenda-se que a comunicação contenha as seguintes informações, disponíveis no formulário de comunicação de incidentes de segurança com dados pessoais da ANPD:

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 9 / 17

7.3. Identificação e dados de contato de:

- 7.3.1. Entidade ou pessoa responsável pelo tratamento.
- 7.3.2. Encarregado de dados ou outra pessoa de contato.
- 7.3.3. Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

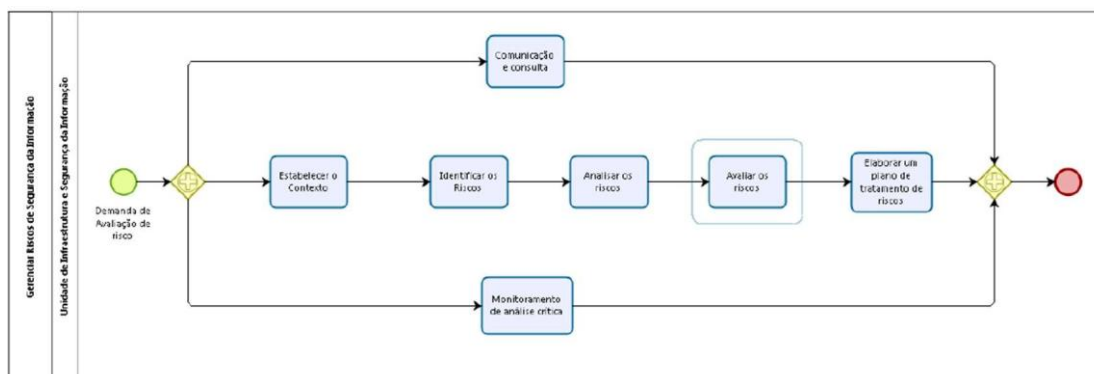
7.4. Informações sobre o incidente de segurança com dados pessoais:

- 7.4.1. Data e hora da detecção.
- 7.4.2. Data e hora do incidente e sua duração.
- 7.4.3. Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros.
- 7.4.4. Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados
- 7.4.5. Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.
- 7.4.6. Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- 7.4.7. Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.
- 7.4.8. Resumo das medidas implementadas até o momento para controlar os possíveis danos.
- 7.4.9. Possíveis problemas de natureza transfronteiriça.
- 7.4.10. Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

7.5. Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente.

7.6. No momento da comunicação preliminar deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las. A ANPD também poderá requerer informações adicionais a qualquer momento.

8. Dos Procedimentos a serem adotados



8.1. Todo e qualquer incidente que se caracterize como uma crise (extrema severidade) deve seguir o Plano de Mitigação de Riscos, elaborados por todos os setores antes do início de qualquer projeto.

8.2. Os eventos de incidente de segurança da informação devem ser categorizados e classificados através de uma matriz de severidade com intuito de se ter uma melhor visibilidade, tratamento e prioridade quanto a sua gestão.

8.3. No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

8.4. Todos os eventos de incidente de segurança da informação devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento.

8.5. A Gestão de Incidentes de Segurança da Informação deve contemplar processos que atendam aos seguintes objetivos:

8.5.1. **Deteção:** identificação de incidentes por meio de monitoração, relatórios, denúncias, informações obtidas de áreas parceiras ou qualquer outra análise de eventos adversos;

8.5.2. **Registro e análise:** registro dos incidentes, análise, classificação quanto ao tipo, severidade e priorização;

8.5.3. **Comunicação:** comunicação do incidente às partes envolvidas e caso necessário entidades externas;

8.5.4. **Resposta:** contenção do incidente, análises forenses, custódia de evidências, tratamento do incidente e da causa raiz;

8.5.5. **Finalização:** encerramento formal e análise pós mortem para identificação de possíveis melhorias em processos, controles e na própria Gestão de Incidentes.

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 11 / 17

8.6. É de extrema importância que o horário de servidores e equipamentos de redes estejam sincronizados com uma fonte confiável de tempo (ex: via protocolo NTP) para que não haja disparidades na correlação de eventos, logs e outros dados.

8.7. Incidentes de segurança podem ser identificados por processos de monitoração da área de infraestrutura por Colaboradores que observem fragilidades, anomalias e violações que coloquem a segurança da empresa em risco.

8.8. Todos os incidentes de segurança da informação devem ser documentados, classificados, priorizados de acordo com a criticidade do Grupo Patense e comunicados aos gestores responsáveis no momento apropriado.

8.9. A investigação de incidentes de Segurança da Informação deve ser realizada exclusivamente pelas áreas de Gestão de Riscos/Infraestrutura e Privacidade de Dados, de forma a garantir a privacidade e o sigilo das informações obtidas.

8.10. Sendo necessárias informações ou levantamentos, para os quais devam ser analisadas trilhas de auditoria (logs), acessos à Internet, fluxo de mensagens ou conteúdo de caixas de correio, ou outras informações que coloquem em risco a privacidade de colaboradores e o sigilo das informações do Grupo Patense, deve ser aberto um incidente junto a área de Gestão de Risco e Privacidade de Dados para que este realize as investigações.

8.11. As informações obtidas e arquivadas pelo processo de Gestão de Incidentes de Segurança da informação devem ser protegidas de forma a garantir a privacidade de colaboradores e o sigilo das informações do grupo, não podendo ser fornecidas a outros departamentos ou auditorias.

8.12. A identificação de incidentes de segurança pode ocasionar o corte imediato dos acessos de colaboradores envolvidos ou a desconexão de sistemas, até que sejam concluídas as investigações necessárias.

8.13. O acesso às evidências e relatório de incidentes de segurança da informação é permitido apenas a área de Gestão de Risco, Privacidade de Dados e aos Gestores diretamente envolvidos nos incidentes.

8.14. A documentação de incidentes, resultados de investigações, evidências e suas soluções devem ser atualizadas logo após a conclusão do tratamento do incidente.

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 12 / 17

8.15. O contato para a notificação de incidentes de segurança da informação deve ser feito diretamente ao Setor de Tecnologia da Informação e se envolver dados pessoais ao Encarregado de Proteção de Dados através de canais previamente definidos.

8.16. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nas demais normas regulamentares.

9. Em que situação e o que comunicar ao titular dos dados?

9.1. Deve ser definido um plano de comunicação de incidentes de segurança da informação que esteja de acordo com a classificação e o nível de criticidade do incidente.

9.2. Em casos mais simples e de baixa criticidade apenas o gestor responsável pelo recurso ou informação deve ser comunicado.

9.3. Em casos mais graves a Controladora, os setores de Segurança da Informação, Privacidade de Dados, jurídico ou outros departamentos pertinentes devem ser comunicados.

9.4. Sempre que o incidente de segurança possa acarretar um risco ou dano relevante aos titulares afetados.

9.5. Critérios mais objetivos serão objeto de futura regulamentação e não poderão ser aqui exigidos sob pena de se inovar na LGPD. De toda forma, pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

9.6. A Controladora deverá avaliar internamente, juntamente com o Encarregado de Proteção de Dados, a relevância do risco ou dano do incidente de segurança para determinar se deverá comunicar à ANPD e ao titular. Para tanto, sugere-se responder internamente às seguintes perguntas:

a. Ocorreu um incidente de segurança relacionado a dados pessoais?

1. Sim – Próxima pergunta.

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 13 / 17

2. Não – Não é necessário comunicar a ANPD se não houve incidente de segurança relacionado a dados pessoais.

b. Existe um risco ou dano relevante aos direitos e liberdades individuais dos titulares afetados em razão do incidente de segurança?

1. Sim – Comunique à ANPD e ao titular.
2. Não – A comunicação à ANPD não será necessária se o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

10. Qual o prazo para comunicar um incidente de segurança para a Autoridade Nacional de Proteção de Dados?

10.1. A LGPD determina que a comunicação do incidente de segurança seja feita em prazo razoável (art. 48, § 1º), conforme será definido pela ANPD. Embora não tenha havido regulamentação nesse sentido, a realização da comunicação demonstrará transparência e boa-fé e será considerada em eventual fiscalização.

10.2. Enquanto pendente a regulamentação, recomenda-se que após a ciência do evento adverso e havendo risco relevante, a ANPD seja comunicada com a maior brevidade possível, sendo tal considerado a título indicativo o prazo de **02 (dois) dias úteis**, contados da data do conhecimento do incidente.

10.3. Tal interregno foi estabelecido com parâmetro na definição de comunicação já existente no Decreto nº 9936/2019 e em virtude da necessidade de gerenciamento dos incidentes de segurança com dados pessoais por parte da ANPD e das consequências danosas que podem ocorrer em razão do atraso nas ações de contenção ou mitigação.

10.4. Reforçamos que o Encarregado pela Proteção de Dados é o responsável pelo contato com a ANPD e qualquer dúvida deve ser direcionada ao e-mail lgpd@patense.com.br.

11. Responsabilidades

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

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 14 / 17

- Condução do processo de Gestão de Incidentes de Segurança da Informação;
- Investigação de incidentes, levantamento, cadeia de custódia e segurança das evidências;
- Acompanhamentos dos planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;
- Comunicação aos Gestores responsáveis, Encarregado de Proteção de Dados;
- Realização de análises pós-incidentes para identificação e tratamento de causas raiz e aprimoramento de processos da empresa e do próprio processo de gestão de incidentes de segurança da informação.

11.2. Colaboradores

- Informar imediatamente à área de Gestão de Riscos e ao Encarregado de Proteção de Dados todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

11.3. Área de Infraestrutura e Desenvolvimento

- Provimento dos acessos necessários para que a área de Gestão de Risco possa realizar a identificação e investigação de incidentes de segurança;
- Responsável pelo provimento de trilhas de auditoria e evidências para a investigação de incidentes;
- Suporte às investigações através do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

11.4. Encarregado de Proteção de Dados

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências
- Receber comunicações da autoridade nacional e adotar providências
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 15 / 17

11.5. Gestores

- Deverá comunicar à ANPD, por meio de seu Encarregado de Proteção de Dados, e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
- Recomenda-se que os controladores adotem posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Ressalte-se, ainda, que eventual e comprovada subavaliação dos riscos e danos por parte dos controladores pode ser considerada descumprimento à legislação de proteção de dados pessoais.
- Embora a responsabilidade e a obrigação pela comunicação à ANPD sejam do controlador, caso excepcionalmente sejam apresentadas informações pelo operador, serão devidamente analisadas pela ANPD.
- As responsabilidades da área Jurídica são: Suporte às questões legais relacionados a incidentes de segurança da informação, quando solicitados.

12. Sanções

12.1. 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.

12.2. 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.

13. Anexos

Anexo I - Termo de Consentimento da Política de Gestão de Incidentes de Segurança da Informação.

14. Referências

- Política de Segurança da Informação;
- Política de Privacidade de dados;
- Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 16 / 17

15. Disposições finais

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

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

15.3. 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.

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

15.5. 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.

16. Histórico de Revisões

Data	Nº Versão	Item revisado	Descrição da revisão
07/07/2021	00		Elaboração da política
04/03/2022	01	Geral	Revisão da política
11/12/2023	02	Geral	Colocação no modelo padrão de governança
Emissor	Nome		Função
	Poliana C Gonçalves		Assistente de Governança Corporativa
Revisor	Nome		Função
	Aline Pelet		Compliance Officer
29/01/2026	Denise Vilaça		Gerente Adm e Compliance Corporativo
Aprovador	Nome		Função
	Rogerio Rocha		Gerente de TI

	Política de Gestão de Incidentes de Segurança da Informação	Nº DOCUMENTO CORP.TI.POL.002
		DATA DE EMISSÃO 01/07/2021
		VERSÃO 02
		PÁGINA 17 / 17

Anexo I

TERMO DE CONSENTIMENTO DA POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. O colaborador abaixo nominado declara, para os fins de Direito, livre de qualquer impedimento.

2. O colaborador abaixo nominado declara ter recebido, lido e concordado com todas as normas estabelecidas neste documento, autorizando esta versão de documento e demais que possam vir, por este ato, a Patense, a monitorar qualquer atividade computacional e de telefonia realizada, em especial os e-mails e as ligações telefônicas geradas ou recebidas através dos terminais telefônicos da empresa, além de inventariar periodicamente o histórico de e-mails, ligações efetuadas, recebidas e outros itens correlacionados.

Eu, _____, declaro estar ciente dos termos das políticas de segurança relacionadas neste documento e autorizo o monitoramento de minhas atividades computacionais e de telefonia pela Patense, estando ciente dos meus direitos, obrigações e deveres para com esta empresa.

_____, _____ de _____ de _____.