cinépolis

Plano de Resposta e Remediação a Incidentes de Privacidade

Versão	Data
1.0	01/01/2024

1. Objetivo

Este Plano de Resposta e Remediação a Incidentes de Privacidade ("Plano") define as etapas a serem observadas por Cinépolis Operadora de Cinemas do Brasil Ltda. ("Cinépolis") na identificação ou recebimento de notificação de uma violação, potencial ou confirmada, de Proteção de Dados Pessoais. Ele é projetado para garantir a implementação de uma abordagem consistente e eficaz para gerenciamento de incidentes de segurança da informação e incidentes de privacidade, estes definidos de forma ampla na Lei Federal n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou "LGPD").

O objetivo deste Plano é conter quaisquer violações, minimizar os riscos associados e garantir que sejam endereçadas as ações necessárias para proteger os Dados Pessoais e evitar novas violações.

Uma resposta eficiente a incidentes envolve todas as áreas da Cinépolis, incluindo suporte de TI, todo o corpo jurídico e operações de negócios. É importante que você leia e compreenda sua função.

Este plano será atualizado sempre que necessário para refletir a Cinépolis em mudanças, novas tecnologias e novos requisitos de conformidade que informam nossa estratégia de segurança cibernética. A Cinépolis executará testes regulares de modo a capacitar seus colaboradores para uma resposta eficaz a incidentes.

2. Referências

O presente Plano deve ser interpretado e aplicado em consonância com as seguintes referências:

(i) LGPD;
(ii) Glossário – Privacidade e Proteção de Dados Pessoais;
(iii) ABNT NBR ISO/IEC 27001:2022;
(iv) ABNT NBR ISO/IEC 27002:2022;
(v) ABNT NBR ISO/IEC 27701:2019.

3. Incidentes de Privacidade

Um Incidente de Segurança da Informação é qualquer evento, independentemente de abrangência ou projeção, que possa comprometer os pilares de segurança da informação, quais sejam confidencialidade, integridade e disponibilidade.

Portanto, qualquer evento que implique o acesso não autorizado aos dados ou informações que utilizamos em nossas atividades (perda de confidencialidade), a perda ou adulteração de quaisquer das informações (perda de integridade) e/ou a perda de acesso parcial ou total às nossas informações ou sistemas (perda de disponibilidade) será considerado um Incidente de Segurança da Informação.

Apenas serão considerados Incidentes de Privacidade aqueles em que Dados Pessoais estejam envolvidos, podendo resultar, por exemplo, de:

- Acesso por terceiros não autorizados (como um hacker) a Dados Pessoais;
- Divulgação não autorizada de Dados Pessoais (como envio para um destinatário incorreto);
- Perda ou roubo de dispositivos de computação contendo Dados Pessoais;
- Indisponibilidade prolongada de um sistema em razão de um incidente de sequestro de dados;
- Alteração ou modificação não autorizada de Dados Pessoais; e
- Perda de disponibilidade, criptografia não autorizada etc.

Além disto, a LGPD adota um texto protetivo e abrangente em seu art. 46, ampliando as situações em que Incidentes de Privacidade podem ser caracterizados, como nos casos em que haja a violação ao regime de Proteção de Dados Pessoais com o Tratamento de Dados Pessoais em desacordo com a Legislação de Privacidade.

Se constatadas evidências de um potencial ou materializado Incidente de Segurança da Informação, a Cinépolis deverá adotar providências imediatas de modo a verificar se também se trata de um Incidente de Privacidade e, em caso afirmativo, iniciar os procedimentos para resposta, remediação e avaliação de suas circunstâncias e gravidades, incluindo, se necessário, informar a Autoridade Nacional de Proteção de Dados (ANPD), e Titulares cujos Dados Pessoais tenham sido comprometidos.

Importante salientar que nem todo Incidente de Privacidade deve ser comunicado à ANPD e/ou Titulares. Caberá à Cinépolis avaliar os riscos e impactos aos Titulares de Dados Pessoais decorrentes do Incidente de Privacidade, e verificar a necessidade de realizar a comunicação.

4. Etapas a serem seguidas em caso de Incidente de Privacidade

A Cinépolis deverá observar as principais etapas abaixo se constatada a ocorrência de Incidente de Privacidade.

(a) ***Investigação, contenção, recuperação e limitação de danos***. As etapas ora mencionadas devem ser executadas para investigação e contenção do possível Incidente de Privacidade e, uma vez confirmado, as ações terão como objetivo o encerramento, recuperação e proteção dos Dados Pessoais comprometidos. Como parte do plano de contenção e recuperação, a Cinépolis deve:

- garantir que todos os dados e hardware potencialmente comprometidos sejam rapidamente preservados para fins de prova e coleta de evidências técnicas para entendimento da causa-raiz do evento e demais circunstâncias, bem como providências de eventual responsabilização

- investigar e documentar se houve de fato um Incidente de Privacidade e, em caso afirmativo, o que é conhecido até o momento, incluindo as categorias de Dados Pessoais afetadas, as categorias de Titulares afetados, os países envolvidos, a maneira pela qual o ocorreu a violação de Dados Pessoais e as medidas disponíveis para conter, deter e remediar o Incidente de Privacidade

- considerar, por exemplo:

(i) como a análise forense pode ajudar a identificar a fonte e a natureza do Incidente de Privacidade

(ii) se há etapas investigativas que possam identificar tentativas de uso ou publicação de quaisquer informações obtidas, especialmente *online* (por exemplo, na *dark web*) e

(iii) se existem quaisquer medidas que possam ajudar os Titulares afetados a se protegerem, por exemplo, com relação ao possível uso indevido de informações obtidas sem autorização.

- identificar o escopo do Incidente de Privacidade. Por exemplo, se um colaborador foi alvo de um ataque de e-mail de *phishing*, será necessário verificar se outros receberam e-mails semelhantes, adotar medidas para bloqueio futuro de e-mails correlatos e conscientizar os colaboradores.

(b) ***Avaliação de risco e impacto do Incidente de Privacidade***. Deve-se verificar se o Incidente de Privacidade pode acarretar risco ou dano relevante aos Titulares. O risco em questão é o risco de a violação de Dados Pessoais, se não for tratada de maneira adequada e oportuna, resultar em prejuízos aos Titulares de Dados Pessoais, tais como em danos físicos, materiais ou não materiais aos indivíduos, incluindo, sem limitação, perda de controle sobre seus Dados Pessoais ou limitação de seus direitos, discriminação, roubo ou fraude de identidade, perda financeira, reversão não autorizada de dados pseudonimizados, danos à reputação, perda de confidencialidade de Dados Pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa para os Titulares em questão. A avaliação destas questões deve ser documentada, seja para respaldar os próximos passos na gestão do evento, seja para respaldar eventuais lições aprendidas em decorrência do evento.

(c) ***Notificação à ANPD***. A ANPD deverá ser notificada sobre o Incidente de Privacidade em caso de: (i) confirmação de sua ocorrência pela Cinépolis; (ii) envolvimento de Dados Pessoais sujeitos à LGPD; e (iii) risco ou dano relevante aos Titulares, a ser apurado conforme item (b) descrito acima.

A notificação à ANPD deverá ocorrer o mais breve possível, em até 2 (dois) dias úteis a contar da ciência do fato, e abordar:

- Natureza do reporte (se completo, preliminar ou complementar);
- Avaliação do risco associado ao Incidente de Privacidade conduzida pela Cinépolis;
- Como a Cinépolis tomou conhecimento do Incidente de Privacidade;
- Data ou período do Incidente de Privacidade, da ciência, da comunicação à ANPD e aos Titulares (se aplicável). Caso a comunicação não se dê no prazo recomendado de 2 (dois) dias úteis, deverão ser indicados os motivos da demora;
- Quantidade de Titulares afetados;
- Existência de comunicação aos Titulares sobre o Incidente de Privacidade e forma adotada;
- Quantidade de Titulares comunicados individualmente. Caso não tenham sido comunicados, deverá ser indicada a razão;
- Descrição da natureza do Incidente de Privacidade, dos Dados Pessoais e Dados Pessoais Sensíveis afetados;
- Categoria de Titulares afetados, destacando inclusive Titulares considerados vulneráveis (crianças, adolescentes e idosos, por exemplo);
- Indicação de medidas técnicas e de segurança utilizadas para a proteção dos Dados Pessoais, observados os segredos comercial e industrial;
- Riscos relacionados ao Incidente de Privacidade e existência de Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
- Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do Incidente de Privacidade;
- Como os Dados Pessoais foram afetados (considerando confidencialidade, integridade e disponibilidade);
- Prováveis consequências e impactos do Incidente de Privacidade aos Titulares;
- Medidas de segurança implementadas para proteger a identidade dos Titulares antes e depois do Incidente de Privacidade;
- Aplicabilidade de regulação setorial em proteção de dados e segurança da informação.

Se não for possível fornecer todas essas informações na notificação inicial, as informações podem ser fornecidas em fases, sem atrasos indevidos, juntamente com os motivos da demora. A complementação deverá ser encaminhada em no máximo 30 dias corridos contados da comunicação preliminar.

A Cinépolis deve estar ciente da necessidade de adotar medidas para gerenciar os riscos contínuos associados à violação de dados pessoais, mesmo após qualquer notificação à ANPD.

(d) ***Notificação aos Titulares.*** A Cinépolis deverá avaliar a necessidade de comunicação tendo em vista a possibilidade de o Incidente de Privacidade acarretar dano ou risco relevante aos Titulares. Referida avaliação deve considerar, dentre outros aspectos:

- O contexto da atividade de tratamento de Dados Pessoais, seguindo a finalidade descrita no mapeamento de Dados Pessoais;
- As categorias e quantidades de Titulares afetados identificados a partir da identificação do fluxo de dados envolvido no incidente;
- Os tipos e quantidade de Dados Pessoais violados por meio procedimento interno para levantamento dos dados pessoais existentes (e.g., uso de *data discovery*);
- Os potenciais danos materiais, morais, reputacionais causados aos Titulares identificados de acordo com os riscos indicados para o tratamento;
- Se os Dados Pessoais violados estavam protegidos de forma a impossibilitar a identificação de seus Titulares, considerando medidas preventivas na Cinépolis como criptografia, anonimização;
- As medidas de mitigação adotadas pela Cinépolis após o Incidente de Privacidade.

Caso seja reconhecida a necessidade de notificação aos Titulares, a comunicação deverá descrever, em linguagem simples:

- Resumo e data da ocorrência do Incidente de Privacidade;
- Descrição dos Dados Pessoais afetados;
- Riscos e consequências aos Titulares;
- Medidas adotadas pela Cinépolis e as recomendadas aos Titulares para mitigar os efeitos do Incidente de Privacidade, se cabíveis;
- Dados de contato do Encarregado da Cinépolis para que os Titulares possam solicitar informações adicionais a respeito do Incidente de Privacidade.

Eventualmente a ANPD poderá solicitar à Cinépolis a apresentação de cópia do comunicado aos titulares para fins de fiscalização. Para estes casos, não será necessário encaminhar a lista de titulares afetados, ou seus dados de contato para comprovação da comunicação.

(e) ***Comunicações externas.*** Se necessário, a Cinépolis deve colaborar com os departamentos relevantes para garantir que uma estratégia apropriada seja implementada caso relatórios se tornem públicos ou se outras medidas forem adotadas pela ANPD ou pelo(s) Titular(es).

(g) ***Remediação.*** A Cinépolis deve determinar as etapas necessárias para remediar o Incidente de Privacidade e evitar que violações semelhantes se repitam. Deve ser feita uma avaliação da eficácia das políticas, procedimentos e sistemas de segurança existentes com base nas lições aprendidas com a violação de dados, incluindo quaisquer aprimoramentos necessários em relação à conscientização da equipe e às medidas de segurança mantidas pela Cinépolis e seus operadores de dados. Essas determinações e avaliações devem ser documentadas.

(h) ***Lições aprendidas.*** No máximo duas semanas após a remediação do Incidente de Privacidade, deverá ser realizada sua retrospectiva, mediante documentação completa do Incidente de Privacidade e avaliação das providências adotadas para sua contenção, de modo a identificar oportunidades de melhoria.