Política de Incidentes

1. OBJETIVO

Esta Política de Incidentes tem como objetivo estabelecer diretrizes e procedimentos para a prevenção, detecção, resposta e resolução de incidentes relacionados à segurança da informação e incidentes técnicos no sistema **AnalytAI**. Garantimos que todas as ocorrências sejam tratadas com rapidez, transparência e em conformidade com a legislação vigente. Além disso, esta política visa criar um ambiente seguro para a operação do sistema, protegendo a integridade dos dados e garantindo a continuidade dos serviços oferecidos aos clientes.

2. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, fornecedores, clientes e terceiros que utilizam ou têm acesso ao sistema **AnalytAI**. Inclui incidentes relacionados à segurança da informação, como acessos não autorizados, vazamento de dados, tentativas de ataques cibernéticos, e também incidentes técnicos, como falhas no sistema, erros operacionais e indisponibilidade de funcionalidades críticas. A abrangência se estende a quaisquer sistemas integrados ao **AnalytAI**, incluindo serviços de terceiros que processam ou armazenam informações sensíveis. A política também se aplica a dispositivos utilizados para acessar a plataforma, como computadores, dispositivos móveis e servidores.

3. CLASSIFICAÇÃO DE INCIDENTES

Os incidentes serão classificados de acordo com a gravidade e impacto no sistema e nos dados dos clientes:

3.1. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

- **Baixo Impacto**: Pequenos incidentes sem comprometimento da integridade, disponibilidade ou confidencialidade dos dados. Exemplo: tentativa de login mal-sucedida repetida sem impacto relevante.
- **Médio Impacto**: Exposição limitada de dados, vulnerabilidade explorada sem impacto significativo. Exemplo: descoberta de falha de segurança antes de exploração ativa.
- **Alto Impacto**: Vazamento de dados sensíveis, comprometimento da infraestrutura ou ameaças que impactam a continuidade do serviço. Exemplo: ataque cibernético que resulte na indisponibilidade do sistema ou no comprometimento de dados estratégicos.

3.2. INCIDENTES DE ERROS TÉCNICOS E OPERACIONAIS

- **Baixo Impacto**: Pequenas falhas ou erros que não comprometem a usabilidade ou desempenho geral do sistema. Exemplo: lentidão temporária no carregamento de dashboards.
- **Médio Impacto**: Falhas que impactam um subconjunto de usuários ou funções específicas. Exemplo: falha na autenticação de usuários ou erro em módulos específicos.
- **Alto Impacto**: Indisponibilidade total do sistema ou falha que impacta significativamente as operações dos clientes. Exemplo: pane total do servidor ou erro crítico que impede o funcionamento do sistema.

Além disso, os incidentes podem ser categorizados de acordo com a natureza do problema, como falha técnica, erro humano, ataque externo ou incidente de conformidade regulatória.

4. PROCEDIMENTO DE RESPOSTA A INCIDENTES

Os incidentes serão tratados de acordo com as seguintes etapas:

4.1. DETECÇÃO E REGISTRO

- Qualquer usuário que identificar um incidente deve relatá-lo imediatamente ao time de segurança da informação ou equipe técnica responsável por meio dos canais oficiais.
- O incidente será registrado via canal oficial com detalhes como data, hora, descrição, impacto percebido, usuários afetados e possíveis ações já tomadas.
- Em casos graves, um protocolo de resposta emergencial será ativado para mitigar riscos antes mesmo da análise completa.
- O canal oficial para reportar incidentes é **oi@letsbot.com.br**.

4.2. ANÁLISE E CLASSIFICAÇÃO

- O time de segurança da informação ou equipe técnica avaliará a gravidade do incidente e classificará conforme a seção 3.
- Será realizada uma investigação inicial para entender o escopo do impacto e identificar a causa raiz do problema.
- Caso seja um incidente de alto impacto, a equipe gestora será acionada imediatamente, e um comitê de resposta poderá ser formado para gerenciar o caso.

4.3. CONTENÇÃO E MITIGAÇÃO

- Medidas emergenciais serão aplicadas para minimizar os danos e evitar a propagação do incidente.
- O acesso a sistemas comprometidos pode ser temporariamente suspenso, e patches de segurança serão aplicados conforme necessário.
- Caso seja identificado um vetor de ataque ou erro técnico recorrente, ações corretivas serão implementadas para evitar recorrências.

4.4. RESOLUÇÃO E RECUPERAÇÃO

- A equipe técnica atuará para corrigir a vulnerabilidade ou falha e restaurar o funcionamento normal do sistema.
- Caso dados tenham sido comprometidos, será realizada a notificação adequada conforme a legislação vigente.
- Testes de validação serão conduzidos para garantir que o problema foi totalmente resolvido antes da retomada completa das operações.

4.5. ANÁLISE PÓS-INCIDENTE

- Um relatório detalhado será elaborado contendo a causa raiz, ações tomadas, tempo de resposta e recomendações para evitar reincidência.
- As lições aprendidas serão incorporadas aos processos de segurança, e melhorias serão implementadas sempre que necessário.
- Em casos críticos, um plano de melhoria contínua poderá ser definido para reforçar a resiliência do sistema.

5. NOTIFICAÇÃO DE INCIDENTES

Em conformidade com a legislação vigente, incidentes graves que envolvam dados pessoais serão reportados às autoridades competentes e aos clientes afetados dentro do prazo estabelecido pela Lei

Geral de Proteção de Dados (LGPD) e demais normas aplicáveis. Além disso, será mantido um canal aberto de comunicação para fornecer atualizações e esclarecimentos aos clientes impactados.

6. RESPONSABILIDADES

- **Equipe de Segurança da Informação**: Responsável pela investigação, contenção e resolução de incidentes de segurança.
- **Equipe Técnica**: Responsável por incidentes técnicos e falhas operacionais, garantindo a rápida recuperação do sistema.
- **Colaboradores e Fornecedores**: Devem relatar qualquer suspeita de incidente e seguir os protocolos de segurança estabelecidos para minimizar riscos.
- **Gestão do AnalytAI**: Garante a implementação, revisão periódica e melhoria contínua desta política, garantindo alinhamento com as melhores práticas do mercado e exigências regulatórias.

7. SLA DE ATENDIMENTO A INCIDENTES

Para garantir uma resposta eficiente aos incidentes, definimos os seguintes prazos para atendimento:

- **Incidentes de Baixo Impacto**: Análise e resposta inicial em até 8 horas úteis, com resolução esperada em até 48 horas úteis.
- **Incidentes de Médio Impacto**: Análise e resposta inicial em até 4 horas úteis, com resolução esperada em até 24 horas úteis.
- **Incidentes de Alto Impacto**: Análise e resposta imediata, com mitigação em até 2 horas e resolução completa em até 12 horas, sempre que tecnicamente viável.

A equipe de segurança da informação e a equipe técnica acompanharão continuamente a situação e fornecerão atualizações periódicas aos clientes afetados.

8. REVISÃO DA POLÍTICA

Esta política será revisada anualmente ou sempre que houver alterações relevantes na legislação, nos processos de segurança do **AnalytAI** ou na identificação de novas ameaças tecnológicas. A cada revisão, melhorias serão incorporadas para garantir que a política continue eficaz e adequada ao ambiente de riscos vigente.