PLANO DE RESPOSTA A INCIDENTE

1. INTRODUÇÃO

De modo a desenvolver uma capacidade de cibersegurança a IT TECH SOLUTIONS adota as melhores práticas referente a resposta a incidente, criando uma capacidade de antecipar e responder a incidentes que afetem a qualidade e o segredo da informação que circule pelo seu ambiente.

2. OBJETIVO

Este plano de resposta a incidente estabelece o procedimento para identificação, Comunicação, Mitigação, Investigação e Aprendizado sobre incidentes confirmados ou sobre suspeita relacionados a segurança da IT TECH SOLUTIONS.

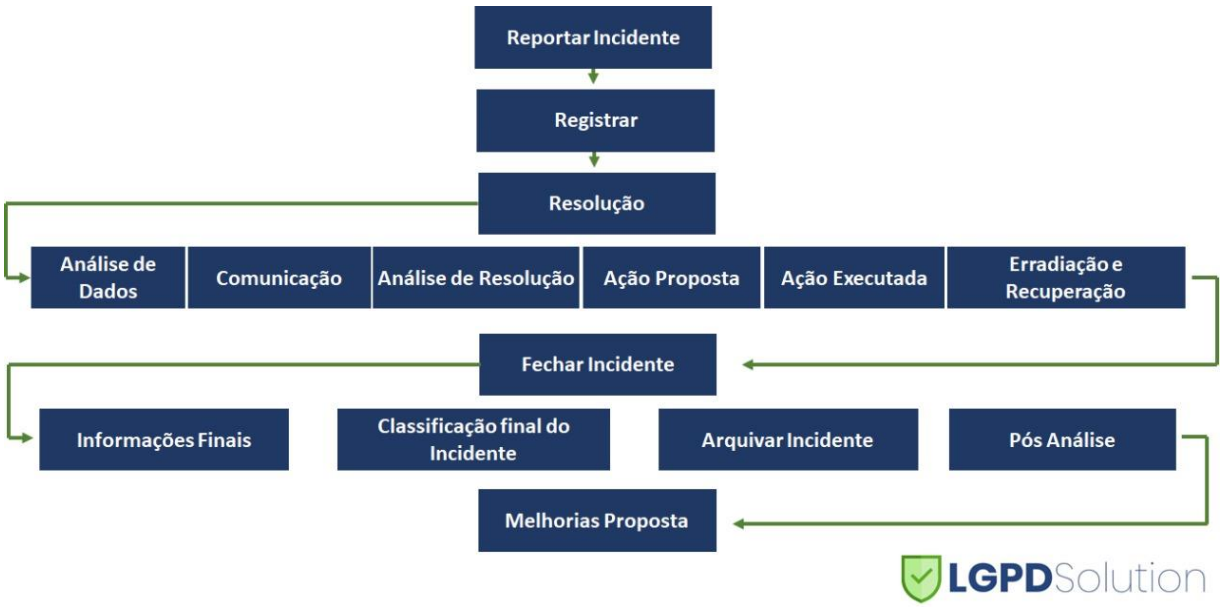
3. ABRANGÊNCIA

Este plano de resposta a incidente da IT TECH SOLUTIONS se aplica a todos os ambientes físicos ou virtuais no qual a empresa armazena, processa ou transmite qualquer informação.

4. PROCEDIMENTO

4.1. Fluxo do Incidente

4.1.1. Todos os alertas recebidos sejam via sistema ou notificação de usuário deve-se seguir o seguinte fluxo:



4.1.2. Descritivo:

4.1.2.1. Reportar Incidente: Compreende como após receber o alerta de possível incidente seja sobre notificação de usuário ou alerta de sistema, os responsáveis pelo tratamento de incidente devem ser alertados para começar as tratativas

4.1.2.2. Registrar: Confirmar o incidente deve ser feito um registro inicial do ocorrido

4.1.2.3. Resolução: Iniciar o processo de tratamento do incidente que inclui:

4.1.2.3.1. **Análise de Dados:** Analisar a notificação recebida ou o alerta do sistema, verificar os logs e os impactos, fazer uma analise de situacional do ambiente entender os impactos e fazer uma pré classificação do incidente:

4.1.2.3.2. **Comunicação:** Se a classificação do incidente for considerada média, comunicar as áreas envolvidas sobre o ocorrido.

4.1.2.3.3. **Análise de Resolução:** Analisar as possibilidades de resolução que terá mais efetividade, menor templo de aplicação e maior segurança

4.1.2.3.4. **Ação Proposta:** Escolher uma ação a ser tomada baseada na análise de resolução.

4.1.2.3.5. **Ação Executada:** Executar ação escolhida

4.1.2.3.6. **Erradicação e Recuperação:** Analisar se o incidente descoberto foi totalmente solucionado, se o ambeinte está totalmente estavel e operacional.

4.1.2.4. Fechar Incidente: Constato que o incidente foi totalmente resolvido fechar o mesmo incluindo as seguintes informações e revisões:

4.1.2.4.1. **Informações Finais:** Descrever os problemas do incidente, medidas totamadas para contornar o problema

4.1.2.4.2. **Classificação final do incidente:** Apontar a classificação final do incidente, se a mesma for diferente da inicial justificar o porque.

4.1.2.4.3. **Pós Analise:** Passado o calor do momento do incidente analisar com mais calma os dados coletados e as informações inseridas e assim fazer os apontamentos necessários para correção tratamento

4.1.2.4.4. **Melhorias Propostas:** Após a última analise definir as melhorias que podem ser feita para evitar que o problema ocorra novamente e para melhorar a resposta ao incidente.

4.2. Identificação

4.2.1. Disponibilizar um meio de comunicação público para que seja notificado sobre possíveis incidentes.

4.2.2. Monitorar constantemente as notificações recebidas.

4.2.3. Ter sistema de monitoramento de ambiente.

4.2.4. Monitorar constantemente os alertas emitidos por esses sistemas e tratá-los adequadamente.

4.3. Comunicação

4.3.1. Após receber notificação ou alerta de possível incidente a equipe de resposta a incidente deve ser acionada seguindo o Anexo I

4.3.2. Caso seja necessário a equipe de resposta incidente pode acionar os responsáveis das áreas afetadas

4.3.3. Caso seja necessária alguma comunicação externa pública acionar o conselho administrativo e a área de Relações Públicas para a elaboração de uma nota/entrevista.

4.3.4. Caso seja necessário a comunicação para algum agente regulador acionar o conselho administrativo para definir a melhor forma de comunicação

4.4. Resolução

4.4.1. Após identificar um incidente deve se fazer uma análise situacional para entender os impactos reais no ambiente e operação, para assim tomar a medida mais assertiva a cada situação.

4.4.2. Analisado o ocorrido e tendo conhecimento do que acontece planejar as ações a serem adotadas

4.4.3. Executar a ação adotada para a correção ou mitigação do incidente

4.4.4. Avaliar e monitorar as ações adotadas e confirmar se elas realmente surtiram efeito

4.4.5. Monitorar o ambiente pelas próximas 24h em caráter crítico

4.4.6. Nenhuma gestão de mudança, sem ser emergencial a segurança ou ao negócio, será permitida nas 24h após o incidente considerado grave

4.4.7. Documentar o incidente ocorrido e as ações tomadas

4.5. Aprendizado

4.5.1. Investigar com mais calma todo o ocorrido desde a notificação/alerta do incidente até a sua resolução

4.5.2. Apontar falhas nas ações tomadas e notificações/alerta realizados no processo

4.5.3. Analisar logs e evidências do ocorrido

4.5.4. Analisar ações tomadas, tempo e impacto dela no ambiente e negócio

4.5.5. Analisar e apontar melhorias no ambiente para que o incidente não volte acontecer ou que tenha menor impacto.

4.5.6. Analisar e apontar melhorias no processo adotado na resolução do incidente.

5. Anexo I

Em caso de incidente acionar os contatos abaixo para o início das tratativas

Usuário	Cargo	Telefone
Paulo Perrotti	DPO – Encarregado de Dados	011 99991-4131

6. REVISÕES

Este plano deverá ser revisado anualmente ou extraordinariamente quando acontecer algum incidente que requeira aperfeiçoamento das medidas adotadas.