Procedimento sobre Tratamento de Incidentes de Segurança da Informação da Alphacode

Versão - Janeiro de 2024

1. Objetivo

Este documento estabelece o procedimento formal para o tratamento de incidentes de segurança da informação na Alphacode, visando assegurar uma resposta coordenada, reduzir danos e prevenir futuras ocorrências.

2. Escopo

Aplica-se a todos os colaboradores, terceiros, fornecedores e qualquer indivíduo que tenha acesso às informações e sistemas de TI da Alphacode.

3. Definição de Incidente de Segurança

Um incidente de segurança da informação é qualquer evento adverso, confirmado ou suspeito, que comprometa a confidencialidade, integridade ou disponibilidade das informações da empresa.

4. Identificação do Incidente

Detecção: Todos os colaboradores são responsáveis por reportar imediatamente qualquer atividade suspeita ou incidente de segurança ao Coordenador de Segurança da Informação (CSI).

Ferramentas de Monitoramento: A equipe de TI deve utilizar ferramentas automatizadas para monitorar e detectar potenciais incidentes de segurança.

5. Reporte de Incidentes

Canais de Reporte: Incidentes devem ser reportados via e-mail para seguranca@alphacode.com.br ou por meio do sistema de tickets interno.

Informações a Serem Incluídas: Descrição do incidente, data e hora de detecção, sistema(s) afetado(s), evidências disponíveis e impacto percebido.

6. Avaliação e Classificação

Avaliação Inicial: O CSI deve avaliar o incidente para determinar a gravidade e o impacto potencial.

Classificação: Incidentes serão classificados como Baixo, Médio ou Alto, com base no impacto à organização, aos clientes e na violação de leis ou regulamentos aplicáveis.

7. Resposta ao Incidente

- **Plano de Resposta**: Para cada classificação de incidente, um plano de resposta específico deve ser executado, incluindo isolamento do sistema, coleta de evidências e comunicação com as partes interessadas.
- **Equipe de Resposta**: Uma equipe de resposta a incidentes será convocada, composta por membros da TI, segurança da informação e, se necessário, recursos humanos e comunicação.

8. Recuperação

- **Restauração dos Serviços**: A prioridade é restaurar os serviços afetados para o estado operacional normal de forma segura.
- **Medidas de Mitigação**: Implementar medidas para prevenir a recorrência do incidente.

9. Comunicação

- **Comunicação Interna e Externa**: Dependendo da gravidade do incidente, a direção e o CSI definirão o nível de comunicação necessária com colaboradores, clientes e autoridades.
- **Relatório de Incidente**: Um relatório detalhado do incidente será elaborado, incluindo causa, resposta, lições aprendidas e recomendações para melhorias futuras.

10. Análise Pós-Incidente

- **Revisão**: Uma revisão pós-incidente será conduzida para avaliar a eficácia da resposta e identificar melhorias nos processos e controles de segurança da informação.
- **Atualização de Políticas e Procedimentos**: As políticas e procedimentos serão atualizados conforme necessário, para refletir as lições aprendidas.

11. Documentação e Registro

Todos os incidentes e ações tomadas devem ser documentados e arquivados para referência futura, auditorias e conformidade legal.