PROCEDIMENTO DE GESTÃO DE DENÚNCIAS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Empresas: Representações Proinde Ltda, Representações Proinde (Belem) Ltda, Representações Proinde (Nordeste) Ltda, Representações Proinde (Norte) Ltda, Representações Proinde (Rio) Ltda.

Versão: 1.0 (Data de emissão: 16 de janeiro de 2026)

Responsável: Oficial de Segurança da Informação (Rogério A. Martins)

1. Objetivo

Estabelecer um mecanismo eficaz e padronizado para o reporte, tratamento e resolução de incidentes de segurança, garantindo a conformidade com normas internas e legais, além de assegurar a proteção ao denunciante.

2. Princípios Fundamentais

• **Confidencialidade:** A identidade do denunciante e as informações do caso são restritas estritamente aos responsáveis pela apuração, com acesso controlado e trilhas de auditoria.

• **Não-Retaliação:** É estritamente proibida qualquer forma de retaliação contra indivíduos que reportem incidentes de boa-fé. Violações a este princípio serão investigadas e punidas disciplinarmente.

3. Escopo de Reporte

Este procedimento aplica-se a todos os colaboradores, estagiários e terceiros. Devem ser reportados eventos como:

• Acessos indevidos, vazamento de dados, *phishing*, engenharia social e *malware*.

• Uso inadequado de credenciais, compartilhamentos irregulares e cópias não autorizadas.

• Descumprimento de políticas, manipulação de logs e condutas antiéticas em segurança.

• Riscos à privacidade e uso indevido de dados pessoais (LGPD).

4. Canais Oficiais de Denúncia

A empresa disponibiliza os seguintes canais, permitindo o anonimato quando tecnicamente viável:

• **E-mail:** seguranca@proinde.com.br

• **Telefone:** +55 13 99640-7097 (Horário comercial, com correio de voz seguro).

• **Formulário Online:** Via website https://sip.proinde.com.br ("Reportar Incidente/Denúncia").

• **Presencial:** Contato direto com o Oficial de Segurança ou representantes do RH/Jurídico.

5. Fluxo do Processo e Prazos (SLA)

Etapa 1: Recebimento e Registro (+1 dia útil)

O responsável deve registrar a denúncia no sistema oficial. Se o denunciante for identificado, deve-se enviar uma confirmação de recebimento contendo o aviso de confidencialidade.

Etapa 2: Triagem e Classificação (até 2 dias úteis)

A equipe de segurança deve qualificar a severidade do incidente e designar a equipe de resposta. A classificação segue os critérios:

• **Alta:** Vazamento confirmado de dados sensíveis, comprometimento de conta privilegiada ou ataque ativo.

• **Média:** Tentativa de *phishing* direcionada, acesso indevido sem exfiltração de dados.

• **Baixa:** Dúvidas, comportamentos atípicos ou pequenas não conformidades.

Etapa 3: Investigação e Resposta

A investigação deve seguir um plano de trabalho documentado, preservando evidências (uso de hash e cadeia de custódia) e respeitando os seguintes prazos de Acordo de Nível de Serviço (SLA):

• **Severidade Alta:** Início em até **4 horas**; Conclusão em **5 dias úteis**.

• **Severidade Média:** Início em **1 dia**; Conclusão em **10 dias úteis**.

• **Severidade Baixa:** Início em **2 dias**; Conclusão em **15 dias úteis**.

Durante esta fase, deve-se aplicar a coleta mínima necessária de dados pessoais para investigar, baseada no legítimo interesse ou obrigação legal.

Etapa 4: Ação Corretiva e Encerramento

As ações incluem conter a ameaça, ajustar acessos e comunicar as partes afetadas. O encerramento exige o registro das lições aprendidas, atualização da base de conhecimento e comunicação do desfecho ao denunciante (se identificado).

6. Documentação e Retenção

Todos os registros, incluindo denúncia, classificação, evidências e ações tomadas, devem ser mantidos por no mínimo **5 anos**, garantindo disponibilidade para auditorias futuras.