opiceblum.com.br
Alameda Joaquim Eugênio de Lima 680 1º andar
01903.001 São Paulo SP Brasil

Modelo de Relatório de Registro de Incidente

1. Introdução

O que deve constar nesse tópico:

- Apresentação: Breve descrição da organização, do sistema afetado e do incidente.
- Objetivos: Definir os objetivos do relatório, como:
    - Documentar o incidente e as ações tomadas (NIST SP 800-61 Revision 2, Seção 7).
    - Analisar as causas do incidente e identificar vulnerabilidades (NIST SP 800-61 Revision 2, Seção 6).
    - Desenvolver recomendações para evitar incidentes futuros (NIST SP 800-61 Revision 2, Seção 6).
    - Cumprir com os requisitos legais e regulamentares, como a LGPD (Lei Geral de Proteção de Dados) (NIST SP 800-171, Seção 3.5.1).
    - Público-alvo (Constituency). Adaptar o relatório ao público-alvo (ex.: alta gerência, equipe técnica, clientes, ANPD) garante a clareza da comunicação e a compreensão das informações (ISO/IEC 27035-2:2023, 6.7)

2. Metodologia de Investigação

O que deve constar nesse tópico:

- Limitação do trabalho (se houver): Descrever quaisquer limitações na investigação, como falta de acesso a dados específicos ou dificuldades de análise forense.
- Ferramentas utilizadas: Listar as ferramentas e tecnologias empregadas na investigação do incidente, incluindo as ferramentas forenses e a sua versão (NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response e ISO/IEC 27041:2018, 5.2.1).

3. Cronologia do Incidente

O que deve constar nesse tópico:

- Data de ocorrência do incidente: Especificar a data e hora precisas do incidente, conforme logs de sistema e outros registros (NIST SP 800-61 Revision 2, Seção 4.1, Resolução CD/ANPD nº 15 de 24 de abril de 2024).

  Recomendação adicional: Utilizar um formato padronizado para registrar a data e hora (ex.: ISO 8601: yyyy-MM-dd'T'HH:mm:ss.SSSZ), incluindo o fuso horário para evitar ambiguidades em casos de equipes ou sistemas distribuídos em diferentes localidades (ISO/IEC 27035-2:2023, B.3.1)

- Data de conhecimento do incidente: Especificar a data e hora em que a organização teve conhecimento do incidente (NIST SP 800-61 Revision 2, Seção 4.2 e Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Datas e atividades realizadas desde a detecção do incidente: Documentar todas as ações tomadas desde a detecção, incluindo isolamento de sistemas, análise forense, recuperação de dados, notificação de autoridades e comunicação com stakeholders (NIST SP 800-61 Revision 2, Seção 5, e Resolução CD/ANPD nº 15 de 24 de abril de 2024).

  Recomendação adicional: Incluir o tempo de resposta para cada atividade realizada (ex.: tempo para isolar os sistemas, tempo para análise forense). A medição do tempo de resposta permite a identificação de gargalos no processo, a otimização das ações e a avaliação da eficiência da equipe. (NIST SP 800-61r2, 4.1.1).

4. Evidências do Incidente

O que deve constar nesse tópico:

- Cadeia de custódia: Documentar a cadeia de custódia das evidências, descrevendo detalhadamente o processo de coleta, armazenamento, acesso e transferência das informações, incluindo os responsáveis por cada etapa. A documentação da cadeia de custódia garante a integridade e a admissibilidade legal das evidências, protegendo-as contra adulteração e questionamentos em eventuais processos legais (ISO/IEC 27037:2015, 5.3).

- Indicação dos documentos e informações relevantes para descrição do incidente: Listar todos os documentos, registros e informações relevantes ao incidente, incluindo logs de sistema, logs de firewall, relatórios de análise forense, mensagens

de e-mail etc. (NIST SP 800-86, LGPD e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

Recomendação adicional: Incluir screenshots, capturas de tela ou outras representações visuais das evidências para complementar a descrição textual (ISO/IEC 27042:2015, 6.3.2).

- Resultado da análise: Detalhar as evidências examinadas e os métodos de coleta utilizados. Descrever também a investigação conduzida no ambiente, como, por exemplo, a análise de um endereço IP desconhecido, e explicar o processo que levou aos resultados finais (NIST SP 800-86).

- Descrição das circunstâncias em que o incidente ocorreu e de como tomou conhecimento: Fornecer um relato detalhado das circunstâncias do incidente e como a organização tomou conhecimento dele, incluindo a fonte da notificação (NIST SP 800-61 Revision 2, Seção 4.2).

- Descrição do impacto do incidente nos sistemas, dados e operações: Descrever o impacto do incidente, incluindo sistemas afetados, dados comprometidos, interrupções de serviço e custos financeiros (NIST SP 800-61 Revision 2, Seção 4.4).

- Causa-raiz e vetor de ataque: Identificar a causa raiz do incidente, o vetor de ataque e as vulnerabilidades exploradas. Fornecer evidências, como mensagens de resgate, alertas de segurança e logs de firewall, para apoiar a análise (NIST SP 800-61 Revision 2, Seção 6.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Descrição dos ambientes/servidores afetados: Especificar os ambientes, servidores e aplicativos afetados pelo incidente (NIST SP 800-61 Revision 2, Seção 4.4).

- Descrição da exfiltração ou da ausência de evidência de exfiltração: Determinar se houve exfiltração de dados e apresentar evidências para sustentar a conclusão (NIST SP 800-61 Revision 2, Seção 4.5 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Natureza e categoria dos dados afetados: Classificar os dados afetados pelo incidente, incluindo informações pessoais, dados financeiros, dados de saúde, etc. (NIST SP 800-171, Seção 3.5.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Número de titulares afetados: Identificar o número de pessoas cujos dados foram potencialmente comprometidos (NIST SP 800-171, Seção 3.5.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Análise de violação das propriedades da informação envolvendo dados pessoais: Realizar uma avaliação das possíveis violações das propriedades da segurança da

informação, envolvendo dados pessoais: confidencialidade, disponibilidade, integridade e autenticidade. (NIST SP 800-171, Seção 3.5.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

5. Medidas Técnicas e Administrativas de Segurança Adotadas

O que deve constar nesse tópico:

- Ações adotadas para tratamento do incidente: Descrever as ações tomadas para conter, mitigar e recuperar do incidente, incluindo isolamento de sistemas, remoção de malware, restauração de dados, aplicação de patches e correções (NIST SP 800-61 Revision 2, Seção 5 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Medidas de segurança técnica e administrativas adotadas antes do incidente: Descrever as medidas de segurança implementadas antes do incidente, como políticas de segurança, controle de acesso, firewalls, antivírus, criptografia e treinamento de funcionários (NIST Cybersecurity Framework, Funções: Identificar, Proteger, Detectar, Responder, Recuperar e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Novas medidas de segurança técnica e administrativas adotadas após o incidente: Descrever as novas medidas de segurança implementadas em resposta ao incidente, incluindo a atualização de políticas, a implementação de novas tecnologias, a revisão de processos e o treinamento adicional de funcionários (NIST Cybersecurity Framework, Funções: Identificar, Proteger, Detectar, Responder, Recuperar e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

- Medidas de correção e de mitigação dos efeitos do incidente para os titulares: Descrever as medidas tomadas para corrigir os efeitos do incidente e minimizar os danos aos titulares, incluindo a recuperação de dados, a notificação dos titulares afetados e a assistência à recuperação e a oferta de serviços (NIST SP 800-171, Seção 3.5.2 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

  Recomendação adicional (apenas para relatórios internos): Detalhar o processo de comunicação com stakeholders (internos e externos), especificando os canais de comunicação utilizados, o conteúdo das mensagens e a frequência dos updates. A comunicação transparente e eficiente com stakeholders é fundamental para a gestão de crises, a manutenção da confiança e o alinhamento das expectativas. (ISO/IEC 27035-1:2023, 4.6)

6. Conclusão sobre Comunicação à ANPD e aos Titulares

O que deve constar nesse tópico:

- Avaliação do risco e possíveis danos aos titulares: Realizar uma avaliação do risco e dos possíveis danos aos titulares, incluindo perda financeira, danos à reputação, violação da privacidade e riscos de criminalidade (ISO/IEC 27035-2:2023, A.11, NIST SP 800-171, Seção 3.5.1 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).
- Se for comunicado: Descrever a forma e o conteúdo da comunicação à ANPD (Autoridade Nacional de Proteção de Dados) e aos titulares, de acordo com os requisitos da LGPD e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024.
- Se não for comunicado: Justificar a decisão de não comunicar, apresentando as razões e as evidências que justificam a decisão (LGPD, Art. 48 e Resolução CD/ANPD nº 15 de 24 de abril de 2024 e Art. 10 da Resolução CD/ANPD nº 15 de 24 de abril de 2024).

7. Considerações Finais

O que deve constar nesse tópico:

- Resumo executivo das informações coletadas e dos exames realizados: Apresentar um resumo conciso das principais informações do relatório, incluindo os principais pontos da investigação, os danos causados, as ações tomadas e as lições aprendidas.
- Síntese sobre dever de comunicação: Reiterar os requisitos legais para comunicação de incidentes de segurança, especialmente no contexto da LGPD, e destacar a importância da transparência e da comunicação com os titulares de dados.

8. Lições Apreendidas

O que deve constar nesse tópico:

- Lições apreendidas: Indicar quais foram as principais lições aprendidas com o incidente (NIST SP 800-61 Revision 2, Seção 4.1.1)

- Prevenção de incidentes: Relacionar as lições aprendidas com as melhorias propostas no plano de ação para garantir a efetividade do aprendizado e a prevenção de incidentes futuros (ISO/IEC 27035-1:2023, 5.6):

9. Responsáveis e assinaturas

Data e Assinatura. Importante que o Relatório seja datado e assinado pelo menos pelo Encarregado pelos dados Pessoais ou responsável designado. (ISO/IEC 27035-1:2023, 4.7.4)

Referências para elaboração deste documento.:

- NIST SP 800-61 Revision 2: Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-86.pdf
- NIST Cybersecurity Framework (CSF): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- ABNT NBR ISO/IEC 27035-1, 27035-2 e 27035-3: https://www.normas.com.br/produto/normas-brasileiras-e-mercosul/pesquisar/27035
- Lei Geral de Proteção de Dados (LGPD): https://www.gov.br/anpd/pt-br/assuntos/legislacao/lei-geral-de-protecao-de-dados
- Resolução CD/ANPD nº 15 de 24 de abril de 2024: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024

O modelo de Relatório de Tratamento de Incidente deve ser adaptado e ajustado de acordo com as características específicas de cada incidente e da organização.

Esse documento foi elaborado pela Equipe de Resposta a Incidentes do Opice Blum, Bruno Advogados Associados.

Tiago Neves Furtado
Vinicius Azevedo Coelho
Guilherme Ochsendorf de Freitas