CODATA	RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Emissão 11-Julho-2024	Classificação Uso interno
Código N-SI-006		Versão 1.1	Aprovado por: DITEC

1. Introdução

1.1. A Norma de segurança da informação **N-SI-006** complementa Política Geral de Segurança da Informação, definindo as diretrizes para responder eventos ou incidentes de segurança estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais da Companhia de Processamento de Dados da Paraíba (CODATA).

2. Propósito

2.1. Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais da CODATA.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Incidentes de segurança da informação

4.1.1. Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da CODATA serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;

4.1.2. Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista e registrada na base de conhecimento e no banco de dados de erros conhecidos da CODATA;

4.1.3. Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados a área de segurança da informação, através da abertura de chamados na central de serviços da CODATA;

4.1.4. A área de segurança da informação deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas como, por exemplo, membros do time de resposta a incidentes de segurança da informação;

4.1.5. Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;

4.1.6. A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;

4.1.7. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

4.2. **Time de resposta a incidentes de segurança da informação**

4.2.1. O time de resposta a incidentes de segurança da informação da CODATA deverá ser composto por, no mínimo, representantes das seguintes áreas:

4.2.1.1. Encarregado de Dados Pessoais;
4.2.1.2. Gerência de Infraestrutura;
4.2.1.3. Gerência de Desenvolvimento;
4.2.1.4. Gerência de Segurança da Informação e Crimes Cibernéticos;

4.2.2. Conforme a natureza do incidente, colaboradores de qualquer setor da CODATA podem ser convocados a participar do time de resposta a incidentes de segurança da informação.

4.3. **Disseminação de informação sobre incidentes de segurança da informação**

4.3.1. Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas à Companhia de Processamento de Dados da Paraíba sem aprovação expressa e formal da diretoria.

5. Papéis e Responsabilidades

5.1. **ENCARREGADO DE DADOS PESSOAIS**

5.1.1. É de responsabilidade do ENCARREGADO DE DADOS PESSOAIS

5.1.1.1. Atuar na resposta aos incidentes de segurança que envolvam dados pessoais ou que possam potencialmente envolvê-los;
5.1.1.2. Em casos de incidentes envolvendo dados pessoais que resultem em risco ou dano considerado relevante aos titulares, deve comunicar à ANPD e ao titular dos dados no prazo de três dias úteis a partir do momento em que teve conhecimento de que o incidente afetou dados pessoais, exceto se houver um prazo específico previsto em legislação aplicável para essa comunicação;
5.1.1.3. Caso não seja possível ter todas as informações, deverá ser enviada uma comunicação preliminar, que serão complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação;
5.1.1.4. Se não for necessária a notificação à ANPD e/ou aos titulares, o Encarregado deve registrar a justificativa no Formulário Interno de Registro de Incidente de Segurança com Dados Pessoais;

5.1.1.5. Poderá elaborar documentos complementares em relação à sua atuação no incidente que envolva dados pessoais ou que possam potencialmente envolvê-los.

5.2. **GERENTE DE SEGURANÇA DA INFORMAÇÃO E CRIMES CIBERNÉTICOS**

5.2.1. É responsabilidade do GERENTE DE SEGURANÇA DA INFORMAÇÃO E CRIMES CIBERNÉTICOS:

5.2.1.1. Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;

5.2.1.2. Comunicar prontamente o time de resposta a incidentes de segurança da informação da CODATA sobre eventos e incidentes de segurança.

5.3. **TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

5.3.1. É responsabilidade do TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:

5.3.1.1. Apoiar a equipe de segurança da informação no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta a incidentes de segurança da informação;

5.3.1.2. Aconselhar a diretoria da Companhia de Processamento de Dados da Paraíba sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.

5.4. **COMUNICAÇÃO**

5.4.1. É responsabilidade da GERÊNCIA DE COMUNICAÇÃO:

5.4.1.1. Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma **N-SI-006** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da Companhia de Processamento de Dados da Paraíba.

8.2. A presente norma foi aprovada no dia 11 de julho de 2024.

ÂNGELO GIUSEPPE GUIDO DE ARAÚJO RODRIGUES– Presidente

EDUARDO PAIVA VARANDAS – Diretor Técnico