NSI-006	**RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**	Data: 14/11/2022 Revisão: Uso Interno
Aprovador: Jose Ribamar Gabriel de Morais Junior		Elaborador: Marcos Johnny Rodrigues Rocha

1. Introdução

1.1. A Norma de Segurança da Informação 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 AJCRED.

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 AJCRED.

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 AJCRED 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 AJCRED;

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 empresa;

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 AJCRED deverá ser composto por, no mínimo, representantes das seguintes áreas:

4.2.1.1. Gerência de Infraestrutura;

4.2.1.2. Gerência de Desenvolvimento;

4.2.1.3. Chefe de Segurança da Informação;

4.2.2. Conforme a natureza do incidente, colaboradores de qualquer setor da AJCRED 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 AJCRED sem aprovação expressa e formal da diretoria.

5. Papéis e Responsabilidades

5.1. CHEFE DE SEGURANÇA DA INFORMAÇÃO

5.1.1. É responsabilidade do CHEFE DE SEGURANÇA DA INFORMAÇÃO:

5.1.1.1. 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;

5.1.1.2. Comunicar prontamente o time de resposta a incidentes de Segurança da Informação da empresa sobre eventos e incidentes de segurança

5.2. TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

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

5.2.1.1. 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. COMUNICAÇÃO

5.3.1. É responsabilidade da GERÊNCIA DE COMUNICAÇÃO:

5.3.1.1. 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 Política

8.1. A presente política foi aprovada no dia 14 de novembro de 2022.

Jose Ribamar Gabriel de Morais Junior

Socio Diretor

Marcos Johnny Rodrigues Rocha

Analista de Sistema