1. O objetivo deste documento é apresentar os critérios para a análise de relevância dos incidentes cibernéticos, utilizados pelo Sicoob.

2. Na Tabela 1, abaixo, são apresentados os detalhes das fases e dos critérios de classificação de relevância de incidente cibernético. Os critérios foram selecionados a partir de *framework* de mercado (Ref. 1 e Ref. 2, citadas no item 4 deste documento) e da experiência anterior com a análise de impacto de negócios, que faz parte do processo de gestão de continuidade de negócios (Ref. 3, citada no item 4 deste documento).

3. *Análise de relevância de incidentes cibernéticos*: a determinação da relevância do incidente possui 4 (quatro) fases, listadas a seguir:

3.1 *1ª fase – Avaliação do incidente cibernético*

a) incidentes relacionados a sistemas de TI geralmente afetam os negócios e as funcionalidades que eles fornecem, resultando em algum impacto negativo para os usuários. A equipe de tratamento de incidentes não deve considerar somente o impacto atual, causado pelo incidente, mas também um provável impacto futuro, caso não seja tratado imediatamente;

b) na primeira etapa de avaliação, os incidentes são classificados sob 4 (quatro) critérios: *criticidade do serviço*, *impacto legal*, *impacto financeiro* e *impacto de imagem*. Cada critério possui peso diferenciado, conforme as tabelas a seguir:

Tabela 1 – Criticidade do Serviço

Criticidade do serviço (impacto na funcionalidade) – Peso 5	
Nenhum – 0	Não afeta a capacidade da organização em fornecer todos os serviços a todos os usuários.
Baixo – 1	Efeito mínimo – a organização ainda pode fornecer todos os serviços críticos a todos os usuários, mas perdeu em eficiência.
Médio – 2	A organização perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários do sistema.
Alto – 3	A organização não pode fornecer alguns serviços críticos a qualquer usuário enquanto não se recuperar do incidente.

Tabela 2 – Impacto Legal - Impacto

Impacto legal (descumprimento de lei/norma) – Peso 2	
Nenhum – 0	Não há impacto legal ou regulatório para a organização.
Baixo – 1	Pode gerar advertência ou multa pecuniária por órgãos reguladores e fiscalizadores externos pelo não cumprimento de leis e normas, e a terceiros ou parceiros por força de contrato.
Médio – 2	Pode gerar, além de advertência e/ou multa, outras sanções administrativas, como rescisão de contrato, suspensão e/ou inabilitação temporária ou permanente para o exercício de cargos de direção na administração ou gerência em instituições financeiras, bem como a impossibilidade de atuação em determinados setores e/ou com determinados produtos, pelo não cumprimento de leis e/ou normas, ou por força de contrato.

Alto – 3	Pode gerar, além das sanções previstas nas respostas anteriores, a cassação da autorização de funcionamento da instituição e/ou detenção e/ou reclusão de executivos, ou a suspensão da efetividade de negócio por força de contrato.

Tabela 3 – Impacto Financeiro

Impacto financeiro (em caso de parada do serviço) – Peso 3 *	
Nenhum – 0	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *insignificante* na *Matriz de avaliação de riscos operacionais* da entidade.
Baixo – 1	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *menor* na *Matriz de avaliação de riscos operacionais* da entidade.
Médio - 2	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *moderada* na *Matriz de avaliação de riscos operacionais* da entidade.
Alto - 3	Em caso de incidente cibernético, a entidade deixa de ganhar ou perde valor menor do que a faixa de valores classificada como *maior ou extrema* na *Matriz de avaliação de riscos operacionais* da entidade.

b.1) como cada entidade possui sua própria matriz de avaliação de riscos, construída com base nos valores de Patrimônio de Referência (PR), em caso de dúvidas quanto à avaliação do impacto financeiro o *Manual de Risco Operacional* deverá ser consultado.

Impacto de imagem (em caso de parada do serviço) – Peso 4	
Nenhum – 0	Não compromete a imagem.
Baixo – 1	O comprometimento é insignificante.
Médio – 2	O comprometimento merece atenção e ações corretivas.
Alto – 3	O comprometimento é significativo/severo.

3.2 *2ª fase – Avaliação da sensibilidade dos dados e das informações envolvidas no incidente*

a) incidentes podem afetar a confidencialidade, integridade e disponibilidade das informações da organização. Incidentes cibernéticos que geram vazamentos de dados pessoais, dados pessoais sensíveis ou confidenciais, por exemplo, são mais relevantes do que incidentes cibernéticos que geram vazamento de dados de uso restrito;

b) na segunda etapa de avaliação de relevância dos incidentes, o responsável pela análise deverá selecionar uma das seguintes opções:

Sensibilidade das informações – Peso 5	
Nenhum – 0	Nenhuma informação foi vazada, alterada, excluída ou comprometida.
Baixa – 1	Informações estão indisponíveis temporariamente.

Média – 2	Informações não sensíveis (sem dados pessoais) foram indevidamente acessadas, vazadas, alteradas ou excluídas.
Alta – 3	Informações pessoais e/ou sensíveis/confidenciais foram indevidamente acessadas, vazadas, alteradas ou excluídas.

3.3 *3ª fase – Avaliação da recuperabilidade do incidente*

a) a capacidade de recuperação de um incidente determina os possíveis procedimentos que a equipe de tratamento deve seguir para o tratamento. Um incidente de alto impacto aos negócios da organização e de fácil recuperação pode ser aquele em que a equipe de resposta a incidentes atue primeiro, tratando e solucionando o incidente. No entanto, pode haver casos de vazamento de dados pessoais em que seria necessário envolver não só pessoas e equipes internas da organização, mas titulares de dados e o órgão de fiscalização (ANPD). Dessa forma, a comunicação e a recuperação podem ser realizadas de forma simultânea. A equipe de tratamento deve priorizar a resposta a cada incidente de acordo com as estimativas de impacto e os recursos e esforços necessários para a sua recuperação;

b) a criticidade do incidente e os tipos de recursos afetados determinarão a quantidade de tempo e os recursos que deverão ser gastos na recuperação desse incidente. Em alguns casos, não é possível recuperar-se de um incidente (por exemplo, se a confidencialidade de informações sensíveis tiver sido comprometida) e não faria sentido gastar recursos limitados em um ciclo prolongado de tratamento de incidentes, a menos que esse esforço fosse direcionado para garantir que um incidente semelhante não ocorra no futuro.

Dificuldade de recuperação do incidente – Peso 5	
Nenhuma – 0	O tempo de recuperação é previsível, com recursos existentes.
Baixa – 1	O tempo para recuperação é previsível, com recursos adicionais.
Média – 2	O tempo para recuperação é imprevisível.
Alta – 3	A recuperação do incidente não é possível (por exemplo: dados confidenciais vazados e publicados)

3.4 *4ª fase – Determinação da relevância do incidente cibernético*

a) a relevância do incidente cibernético é determinada a partir da seleção dos critérios definidos neste documento, considerando os respectivos pesos na fórmula abaixo:

Relevância = (CS*5 + IL*2 + IF*3 + II*4 + SI*5 + RC*5)

CS - Criticidade do serviço
IL - Impacto legal
IF - Impacto financeiro
II - Impacto na imagem
SI - Sensibilidade da informação
RC - Recuperabilidade do incidente

Figura 1 – Fórmula da relevância do incidente cibernético.

b) o resultado da análise da relevância do incidente cibernético é apresentado na tabela abaixo, com a seguinte descrição:

b.1) *Incidente de relevância baixa (Incidente não relevante)*: incidente com impacto baixo/leve, de acordo com os critérios definidos neste documento;

b.2) *Incidente de relevância média (Incidente não relevante)*: incidente com impacto médio/significativo, de acordo com os critérios definidos neste documento;

b.3) *Incidente de relevância alta (Incidente relevante)*: incidente com impacto alto/grave, de acordo com os critérios definidos neste documento. O incidente com esta classificação é considerado relevante para atendimento à Resolução CMN nº 4.893/2021.

Relevância do incidente cibernético	
Baixo = de 0 a 45	**INCIDENTE NÃO RELEVANTE**
Médio = de 46 a 59	**INCIDENTE DE RELEVÂNCIA MÉDIA**
Alto >= 60	**INCIDENTE DE RELEVÂNCIA ALTA**

O resultado **ALTO** classifica o incidente como **RELEVANTE**.

4. Referências:

Computer Security Incident Handling Guide – NIST. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NCCIC Cyber Incident Scoring System. National Cybersecurity and Communications Integration Center. Disponível em: https://www.uscert.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf
Manual de Risco Operacional
*National Cyber Security Centre***.** Disponível em: https://www.ncsc.gov.uk
FBI. *Cyber Incident Reporting*. Disponível em: https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view