# RESOLUÇÃO CRCBA N.º 659, DE 07 DE NOVEMBRO DE 2022.

Institui a Política de Incidentes de Segurança da Informação do Conselho Regional de Contabilidade da Bahia.

O **Presidente do CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA BAHIA,** no uso de suas atribuições legais e regimentais,

Considerando a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico e não digital controlado, eficiente e seguro, de forma a oferecer todas as informações necessárias à classe contábil e à sociedade, com integridade, confidencialidade e disponibilidade;

Considerando a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

Considerando que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta política em relação aos dados pessoais, mesmo após o seu término;

Considerando o relatório de Auditoria de TI com análise e apresentação dos principais pontos de avaliação, recomendação e Diagnósticos de Maturidade em relação as necessidades elencadas em proposta de projeto elaborado para o CRCBA em relação a avaliação de controles COBIT (em suas versões 4.1 e 5),

**R E S O L V E:**

Art.1º Aprovar ad referendum do Plenário, a Política de Incidentes de Segurança da Informação do Conselho Regional de Contabilidade da Bahia, nos termos do Anexo desta Resolução.

Art. 3º A íntegra da Política de Segurança da Informação do CRCBA será disponibilizada em seu Portal e em sua intranet.

Art. 4º Esta resolução entra em vigor após a sua publicação.

ANDRE LUIS BARBOSA DOS SANTOS:79734766520
Assinado de forma digital por ANDRE LUIS BARBOSA DOS SANTOS:79734766520
Dados: 2022.11.08 12:45:25 -03'00'

Contador **André Luís Barbosa dos Santos**
Presidente

| Data | Versão | Elaboração | Aprovação | Descrição |
|---|---|---|---|---|
| 01/04/2021 | 1.0 | Ivanluiz Bastos Trindade | Comitê de Tecnologia | Elaboração do documento |



**INDICE**

## 1. OBJETIVO

Este procedimento tem como objetivo:

- ✓ Garantir a detecção de eventos e tratamento adequado, sobretudo na categorização destes como incidentes de segurança da informação ou não.
- ✓ Garantir que incidentes de segurança da informação sejam identificados, avaliados e respondidos de maneira mais adequada possível.
- ✓ Minimizar os efeitos adversos de incidentes de segurança da informação (tratando-os o mais brevemente possível).
- ✓ Reportar as vulnerabilidades de segurança da informação, além de tratá-las adequadamente.
- ✓ Ajudar a prevenir futuras ocorrências, através da manutenção de uma base de lições aprendidas (Base de Conhecimento – Erros Conhecidos e tratativas de incidentes ou problemas).

## 2. APLICAÇÃO

Este documento estende-se a toda Organização e se aplicável aos clientes, fornecedores e parceiros.

## 3. DEFINIÇÃO

**Incidente de Segurança:** é um ou uma série de eventos não desejados ou não esperados com alta probabilidade de comprometer as operações dos negócios e ameaçar a segurança da informação quanto a Disponibilidade, confidencialidade e integridade;

**Ameaça:** Possível causa potencial de um incidente indesejado, que pode resultar em dano;

**TI:** Tecnologia da Informação;

**SGSI:** Sistema de Gestão de Segurança da Informação;

**RTNC:** Registro de Tratamento de não conformidade;

**Fragilidade:** Caracterizados pelos pontos fracos (sensíveis) da Organização;

**Evento:** são acontecimentos que podem ou não serem planejados.

## 4. RESPONSABILIDADES

- ✓ **Gestor da Qualidade:** Verificar o cumprimento desta norma;

- ✓ **Todos:** Registrar e ou comunicar Incidentes de Segurança da Informação;
- ✓ **Gestor de Serviços:** Auxiliar na análise e tratamento dos incidentes de segurança da informação e analisar e Tratar os incidentes de segurança da informação;

## 5. DIRETRIZES

### Ciclo de vida do incidente de segurança

### Planejamento do Processo

O Planejamento do Processo de Gestão de Incidentes de Segurança da Informação visa que incidentes de segurança sejam sanados rapidamente. Para tal, devemos considerar:

1. Procedimento para Gestão de Incidentes de Segurança da Informação;
2. Matriz de Riscos devidamente atualizada;
3. Fluxo de incidentes de segurança da informação;
4. Estabelecimento da equipe de resposta a incidentes;
5. Planejamento e capacitação da equipe especializada de resposta a incidentes;
6. Conscientização de todos em relação a sensibilidade envolvida com o gerenciamento de incidentes de segurança da informação;
7. Ferramentas de testes e monitoramento; e
8. Ferramenta de registro dos incidentes e eventos.

### Detecção e comunicação

Envolve a detecção (normalmente com a ajuda de ferramentas de automação ou apuração por usuários), coleta de informações associadas e relatórios sobre ocorrências de segurança da informação, vulnerabilidades de segurança que não foram antes exploradas, assim como os incidentes propriamente ditos, sejam eles provocados de forma intencional ou não intencional.

A detecção, comunicação e registro de Incidentes de Segurança da Informação é realizada conforme o Fluxo Gestão de Incidentes.

Todo colaborador ou fornecedor (soluções) que esteja em contato com as informações e/ou os sistemas do CRCBA deve informar quaisquer fragilidades ou eventos que podem levar a um possível incidente de Segurança da Informação.

Imediatamente devem ser informados conforme quadro de escalonamento abaixo, verbalmente ou e-mail informando a descrição do incidente, data e hora ou através do registro do incidente;

### Equipe de Resposta a Incidentes

A equipe de resposta a incidentes de segurança da informação é composta por:

- Técnico de Infraestrutura
- Analista de Segurança da Informação

Todo e qualquer incidente de segurança da informação deve ser informado a equipe de resposta a incidentes respeitando o seguinte escalonamento:

| Nível | Nome | E-mail | Celular |
|---|---|---|---|
| 1 | Litânia Santiago de Azevêdo | dpo@crc-ba.org.br | (71) 9645-8757 |
| 2 | Margarete Santos Luz | diretoria@crc-ba.org.br | (71)99202-4272 |
| 3 | Ramaiana Santos Assis | desenop@crc-ba.org.br | (71) 9915-8021 |

O aprendizado dos incidentes causados por problemas, deve ser registrado na Base de conhecimento ou com uso de fóruns internos. Sempre que necessário, a equipe de Segurança recebe treinamentos ou orientações sobre segurança da informação.
O aprendizado também é compartilhado com as partes interessadas ou envolvidos criando a cultura de lições aprendidas promovendo a conscientização.

**Classificação do Incidente (Impacto)**

O principal objetivo aqui é avaliar os eventos de segurança da informação e decisão sobre se é incidente de segurança da informação.
É preciso realizar uma avaliação das informações relevantes associadas com a ocorrência de eventos de segurança da informação e classificar o evento como um incidente ou não. Sendo este incidente avaliar o impacto do mesmo.

**Baixo:** quando o evento ocorrido não impacta em redundância
**Médio**: Quando aciona a redundância mais não impacta na entrega do serviço;
**Alto:** as medidas redundantes não supriram a demanda, causando impacto na entrega do serviço.

**Classificação do Incidente (Probabilidade)**

**Baixo:** nenhum incidente que afete a disponibilidade, confidencialidade ou integridade da informação ocorreu;
**Médio:** de 1 a 3 incidentes no ano que afetam a disponibilidade, confidencialidade ou integridade da informação;
**Alto:** acima de 3 incidentes que afetam a disponibilidade, confidencialidade ou integridade da informação;

Ao analisar o incidente, também devem ser considerados:

- ✓ bases de dados e procedimentos para investigação, assim como manter estas bases e procedimentos atualizados
- ✓ avaliar a situação com base nas classificações de eventos / incidentes de segurança
- ✓ identificação de serviços afetados
- ✓ mensuração do impactos nos ativos da informação considerando os critérios da informação: confidencialidade, integridade e disponibilidade;
- ✓ priorizar o incidente / evento;
- ✓ reportar o evento / incidente a partes interessadas
- ✓ atribuir as responsabilidades adequadas para o tratamento do incidente / evento
- ✓ outras atividades mais específicas podem ser necessárias para armazenar de forma adequada evidências / provas sobre a causa do incidente (sobretudo em caso de ataques ).

**Priorização e Resolução de incidentes**

Com base na classificação de incidentes de impacto x probabilidade é definida a priorização do incidente e o tempo de resolução.

- **Baixa:** incidente que ocorreu mas não afetou a confidencialidade, integridade ou disponibilidade da informação;
- **Média:** incidentes que ocorrem ou ocorreram com uma certa frequência, mas que não tem um impacto relevante sobre a confidencialidade ou integridade da informação e não podem resultar em não disponibilidade à longo prazo;
- **Alta:** incidentes que ocorrem ou ocorreram com média ou alta frequência que pode resultar em danos relevantes em função da perda da confidencialidade ou da integridade das informações ou que pode resultar em interrupção da disponibilidade das informações e/ou de processos por um período de tempo inaceitável.

Com base na classificação de incidentes é definido o tempo de resolução e a prioridade.

| | **IMPACTO** | | |
|---|---|---|---|
| **URGENCIA** | Alto | Médio | Baixo |
| Alta | Resolução em 2 hrs | Resolução em 4 hrs | Resolução em 2 dias |
| Média | Resolução em 4 hrs | Resolução em 1 dia | Resolução em 3 dias |
| Baixa | Resolução em 5 hs | Resolução em 7 dias | Resolução em 9 dias |

**Nota:** Para incidentes relacionados a terceiros, considerar o SLA ou prazo acordado com o terceiro e informar o cliente quando apropriado (se não tiver um SLA definido, entrar em contato e definir por ocorrência/situação com o fornecedor).

### Tratamento do Incidente e Problemas

Os incidentes deverão ser tratados e documentados conforme este procedimento.

No intuito de identificar a (s) causa (s) raiz e suas potenciais preventivas, os incidentes originados por problemas que causam impacto na Segurança da Informação deverão ser analisados do RTNC, com auxílio da Coordenação da Qualidade e/ou Diretoria, sendo acompanhada e monitorada no Plano de Ação.

### Aprendendo com Incidentes

O Gerente de Serviços deve analisar todos os incidentes registrados com a identificação de tipo e o custo do incidente e, se necessário, deve sugerir ações preventivas (análise de risco) ou corretivas e apresenta-los na reunião de Análise.
Todo tratamento de incidente gerado por problema, deverá ser registrado na base de Conhecimento para se ter um histórico de tratativas, ações a respeito de incidentes de Segurança da Informação.

### Encerramento do Incidente

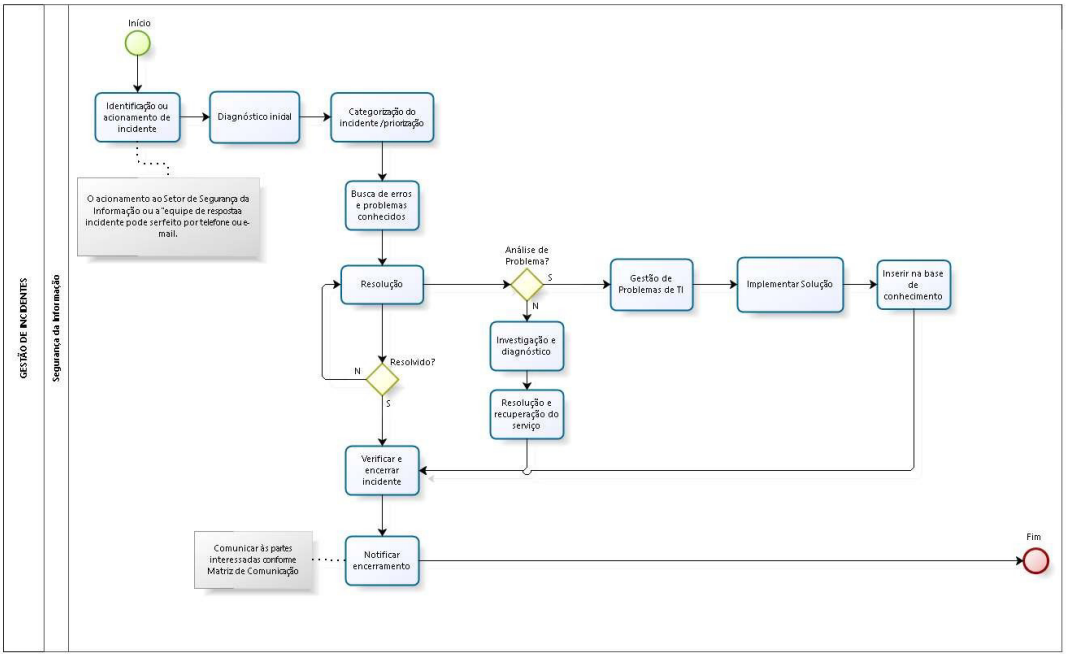
A avaliação de todos os aspectos relacionados ao incidente ocorrido deve indicar os pontos que podem ser melhorados na atividade impactada.

## 6. PENALIDADES

Qualquer descumprimento a este procedimento será considerado uma violação do código de Conduta do CRCBA, e está sujeito a penalidades, de acordo com a CLT -Consolidação das Leis do Trabalho.

## 7. ANEXOS

Fluxo de Gestão de Incidente


GESTÃO DE INCIDENTES
Segurança da Informação
Início
Identificação ou acionamento de incidente
Diagnóstico inicial
Categorização do incidente /priorização
O acionamento ao Setor de Segurança da Informação ou a "equipe de respostaa incidente pode serfeito por telefone ou e-mail.
Busca de erros e problemas conhecidos
Resolução
Análise de Problema?
S
N
Gestão de Problemas de TI
Implementar Solução
Inserir na base de conhecimento
Investigação e diagnóstico
Resolução e recuperação do serviço
Resolvido?
N
S
Verificar e encerrar incidente
Comunicar às partes interessadas conforme Matriz de Comunicação
Notificar encerramento
Fim

**ANEXO II**
**RELATÓRIO DE INCIDENTES**

## DETALHES DO FUNCIONÁRIO

Nome:
Unidade Organizacional:
Contato: (nome e e-mail)

## DESCRIÇÃO DO INCIDENTE

Localização:
Data: DD/MM/AAA Hora: 0X:XX Polícia notificada Sim ( ) Não ( )

Detalhes do Incidente:

Causas do Incidente:

Recomendações:

Acompanhamento de ações:

Atribuído a: Data: DD/MM/AAAA

## REPORTADO POR

Nome: Departamento: