CONSELHO FEDERAL DE CONTABILIDADE
SAUS Quadra 05, Lote 03, Bloco J, Edifício CFC, - Bairro Asa Sul, Brasília/DF, CEP 70070-920
Telefone: - www.cfc.org.br

PORTARIA PRES CFC Nº 102 DE 1º DE SETEMBRO DE 2023.

Aprova norma sobre de Gestão de Incidente de Segurança da Informação.

O PRESIDENTE DO CONSELHO FEDERAL DE CONTABILIDADE, no uso de suas atribuições legais e regimentais, resolve:

Art. 1º Fica aprovada norma, nos termos do Anexo I desta Portaria, sobre de Gestão de Incidente de Segurança da Informação que define as regras gerais para o processo de gestão de incidentes de segurança da informação no âmbito do Conselho Federal de Contabilidade.

Art. 2º Esta Portaria entra em vigor em 17 de agosto de 2023.

CONTADOR AÉCIO PRADO DANTAS JÚNIOR

Presidente

Documento assinado eletronicamente por **Aécio Prado Dantas Júnior**, **Presidente**, em 03/11/2023, às 16:03, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0127913** e o código CRC **98C6A8D5**.

ANEXO I

SGSI

Gestão de Incidente de Segurança da Informação

Elaborado por:	Verificado por:	Aprovado por:
Francisco Edivar	Vanessa Motta	Elys Tevania
Gerente de SI	Apoio à Diretoria	Diretora Executiva

1. Objetivo

Complementar a Política de Segurança da Informação e definir as regras gerais para o processo de gestão de incidentes de segurança da informação no CFC.

2. Referências

ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código de prática para gerenciamento de segurança da informação

ISO/IEC 27001:2013 Tecnologia da informação – Técnicas de segurança – Sistemas de gerenciamento de segurança da informação – Requisitos

3. Responsabilidade

A Alta Direção do CFC é responsável pela viabilização das condições necessárias para a devida aplicabilidade desta norma; já a área de Segurança da Informação é responsável pela atualização desta norma.

A segurança da informação pretendida pelo CFC é de responsabilidade de todos, porém algumas equipes e/ou funções específicas possuem deveres e responsabilidades especiais para o gerenciamento, manutenção e melhoria do SGSI e deste processo de gestão de incidentes de segurança da informação, sendo:

I. Diretoria Executiva: viabilizar condições e recursos para que esta norma seja aplicada integralmente;

II. Comitê de Segurança da Informação (CSI): reunir-se periodicamente para análise crítica do processo, sugerir melhorias e ouvir partes interessadas;

III. Segurança da Informação: Responsável por receber e gerir incidentes de segurança da informação, e pela comunicação do processo aos colaboradores do CFC, para que estes atendam às medidas necessárias em caso de incidentes de segurança:

a) Receber todos os incidentes e/ou eventos de segurança da informação;

b) Determinar a criticidade e priorização do tratamento dos incidentes e/ou eventos de segurança da informação;

c) Aconselhar a área de Comunicação e Tecnologia da Informação sobre quais informações de incidentes e/ou eventos de segurança da informação do CFC podem ser divulgadas para públicos internos e externos;

d) Comunicar prontamente a equipe de tratamento de incidentes sobre todo incidente e/ou evento de segurança da informação;

e) Apoiar as áreas internas do CFC 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;

f) Disponibilizar meio de contato para comunicação de incidentes e/ou eventos de segurança da informação através do canal: http://helpdesk.cfc.org.br/helpdesk/

g) Identificar e envolver outras áreas como: CGTI, COREG, CDPROF, COFIS, COTEC, DEGEP. DEPES, COLOG,

COAD, PROJUR, DELIC, conforme apropriado para a situação.

IV. Tecnologia da Informação

a) Garantir ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;

b) Solucionar situações adversas e acompanhar andamento de solicitações críticas;

c) Possuir conhecimento em tecnologias, serviços e ferramentas suportadas pelo CFC, necessárias para resolução dos incidentes e/ou eventos de segurança da informação.

V. Todos os colaboradores do CFC:

São responsáveis por comunicar qualquer incidente no ambiente físico ou sistêmico por meio do canal: http://helpdesk.cfc.org.br/helpdesk/

a) Informar detalhes do incidente;

b) Quando requisitado, participar de testes de possíveis soluções para incidentes;

c) Contribuir com possíveis intervenções, alterações e/ou melhorias no ambiente de trabalho necessário para solução de incidentes; e

d) Validar o retorno efetivo da operação do processo/serviço afetado.

Observação: Todo incidente de segurança da informação é de classificação confidencial e não deve ser divulgado, preservando os detalhes do ocorrido dentro das áreas responsáveis. Exceções, como em caso de incidentes que impactem clientes, devem ser avaliadas pela área de segurança da informação e reportado para as partes interessadas através dos canais formais estabelecidos.

4. Definições

Consulte o Manual de Terminologia do SGSI.

5. Etapas do gerenciamento de incidentes

Para garantir a efetividade no gerenciamento dos incidentes, o CFC adota o seguinte procedimento:

a) **Identificação**: Etapa onde o incidente de segurança é inicialmente detectado e reportado para a equipe de Segurança da Informação, por meio do canal: http://helpdesk.cfc.org.br/helpdesk/

b) **Registro**: Após o incidente de segurança da informação ser reportado, deve ser prontamente avaliado e discutido para as devidas ações e tratativas;

c) **Classificação**: A área de Segurança da Informação deve classificar e priorizar o incidente de acordo com sua urgência e/ou impacto, para que o incidente seja tratado de acordo com os níveis de severidade e prazos estipulados pela organização conforme: Tabela 1 - Níveis de severidade dos incidentes e Tabela 2 - Prazo de atendimento dos incidentes;

d) **Investigação e Diagnóstico**: Os departamentos responsáveis por tratar o incidente de segurança da informação devem tomar ações para identificação e resolução do incidente. Durante o diagnóstico e investigação, todas as ações tomadas devem ser registradas em sistema, incluindo:

I. Confirmar o impacto do incidente, incluindo quais e como os usuários são afetados;

II. Identificar eventos que poderiam ter ocasionado o incidente;

III. Pesquisar uma solução em bases de conhecimento locais e/ou das equipes envolvidas.

e) Encerramento: Nesta fase o departamento de Segurança da Informação comunica se o incidente foi completamente solucionado e se o usuário está satisfeito e concorda em encerrar o incidente. Durante o encerramento, todas as ações tomadas devem ser registradas em sistema de incidentes, incluindo:

I . Documentação do Incidente: Validar todos os requisitos de documentação do incidente para confirmar que os registros estão completos, se houver;

II. Problemas Recorrentes: Determinar se existe probabilidade de reincidência do incidente e se é necessário tomar ações preventivas;

III. Encerramento: Formalmente encerrar o incidente e notificar o usuário afetado e todos os envolvidos na plataforma de incidentes ou por e-mail.

6. Níveis de severidade dos incidentes

Nível de Severidade	Descrição
Nível 1 – Alto	Sistema indisponível. Incidentes que resultem em interrupções sérias no sistema de produção, impedindo em absoluto sua utilização. Incidente que resulte em interrupções sérias não programadas no sistema de produção ou que afetem muitos usuários, e que não possibilitem opções alternativas para execução das funções por parte dos usuários. Incidente que resulte em vazamento de dados, seja de clientes ou próprios do CFC. Incidente que resulte em violação de dados, seja de clientes ou próprios do CFC.
Nível 2 – Médio	Incidente em que os utilizadores têm uma forma alternativa de executar as funções, com pouco mais, ou a mesma quantidade de esforço de antes da ocorrência do incidente.
Nível 3 – Baixo	Incidente para o qual há alternativa que permita ao utilizador a execução de suas funções.

7. Prazo de atendimento aos incidentes

	Prazo de Atendimentos dos Incidentes

Níveis de Severidade	Início do Atendimento (Contado a partir registrado via sistema ou e-mail)	Solução de Contorno (Em horas corridas)	Solução Definitiva (Em horas corridas)
Nível 1	Imediato	Consultar PCTI	Consultar PCTI
Nível 2	12 horas	20 horas úteis	48 horas úteis
Nível 3	24 horas	40 horas úteis	120 horas úteis

8. Incidentes

Exemplos de incidentes considerados com Nível 1 de Severidade (Alto):

a) Ataques de negação de serviço;

b) Vulnerabilidade ou varreduras não autorizadas;

c) Acesso interno ou externo não autorizado a informações ou sistemas;

d) Violação significativas das PSI - Política de Segurança da Informação e Normas de segurança da informação; e

e) Perda ou roubo de equipamento levando a exposição potencial de informações não públicas.

Exemplos de incidentes considerados com Nível 2 de Severidade (Médio):

a) O uso inadequado dos sistemas de informação;

b) Códigos maliciosos (vírus, trojan, *rootkits*) que afetem apenas estações em pequena quantidade, ou seja, sem indício de propagação; e

c) A instalação ou ativação de um ponto de acesso sem fio não autorizado.

Exemplos de incidentes considerados com Nível 3 de severidade (Baixo):

a) Equipamentos desbloqueado exibindo informações sigilosas;

9. Lições aprendidas

Para garantir a efetividade das ações no tratamento dos incidentes de Segurança da Informação, bem como para reduzir riscos relacionados, o CFC adota as seguintes ações:

Levantamento de fatos e dados relacionados a incidentes de Segurança da Informação: A Equipe de Segurança da Informação deve levantar e consolidar trimestralmente as informações relacionadas a incidentes de Segurança da Informação, incluindo:

Coletar e atualizar dados da base de conhecimento sobre incidentes e ocorrências de Segurança da Informação;

Realizar reuniões com as unidades organizacionais responsáveis pelo tratamento do incidente (apenas

quando necessário);

Atualizar registros de riscos: Com base no resultado da análise trimestral dos incidentes de Segurança da Informação, a Equipe de Segurança da Informação deve:

Alinhar com gestores de área a necessidade de modificar os níveis de risco atualmente mapeados;

Validar com os gestores de área a necessidade de novos planos de ação para tratamento desses riscos.

Reportar resultados para o CSI: Com base no resultado da análise trimestral dos incidentes de Segurança da Informação, a Equipe de Segurança da Informação deve reportar os resultados para o CSI, incluindo:

Apresentar os dados quantitativos e indicadores relacionados a incidentes de segurança da Informação;

Apresentar análise da efetividade do tratamento de incidentes de Segurança da Informação;

Apresentar recomendações de ações para evitar recorrências de incidentes ou reduzir riscos relacionados à Segurança da Informação.

Eventualmente poderão ser convocados demais envolvidos no tratamento de incidentes de Segurança da informação, para prestar mais esclarecimentos e sugerir ações adicionais.

Analisar resultados e definir ações: Com base nas informações apresentadas pela Equipe de Segurança da Informação, o CSI deve:

a) Analisar os resultados apresentados;

b) Definir quais ações devem ser implementadas para evitar recorrências de incidentes ou reduzir riscos relacionados à Segurança da Informação.

10. Controle de revisões

Revisão	Item	Alteração	Data
0	-	Versão inicial	19/06/2023