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 103 DE 1º DE SETEMBRO DE 2023.

Aprova norma sobre Responsabilidades 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, que define responsabilidades específicas dos colaboradores do CFC para garantir que suas funções perante a segurança da informação sejam realizadas conforme os requisitos definidos na Política de Segurança da Informação (PSI).

Art. 2º Esta Portaria entra em vigor em 4 de setembro de 2023.

CONTADOR AÉCIO PRADO DANTAS JÚNIOR

Presidente

Documento assinado eletronicamente por **Aécio Prado Dantas Júnior**, **Presidente**, em 01/09/2023, às 15:14, 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 **0127924** e o código CRC **10159AB2**.

ANEXO I

SGSI

Responsabilidades 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

Apresentar as responsabilidades específicas dos colaboradores do CFC para garantir que suas funções perante a segurança da informação sejam realizadas conforme os requisitos definidos na Política de Segurança da Informação (PSI).

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. Definições

Consulte o Manual de Terminologia do SGSI.

4. Responsabilidades

A Alta Direção do CFC é responsável pela viabilização das condições necessárias à devida aplicabilidade desta norma, e o Comitê de Segurança da Informação (CSI) 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 bom gerenciamento, a manutenção e a melhoria do SGSI e do processo de proteção da informação, sendo:

1. Alta Direção

A Alta Direção deverá viabilizar condições e recursos para que esta norma seja aplicada integralmente.

2. Comitê de Segurança da Informação (CSI)

O Comitê de Segurança da Informação deverá cumprir as seguintes responsabilidades dentro da organização:

I – assessorar a implementação das ações de segurança da informação;

II – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III – participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV – propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação; e

V – deliberar sobre normas internas de segurança da informação.

3. Departamento de Segurança da Informação

O Departamento de Segurança da Informação é responsável por:

I – submeter ao CSI as versões da Política e das Normas de Segurança da Informação, e, após a aprovação, publicar e promover sua divulgação aos colaboradores do CFC;

II – propor métodos e processos específicos para a segurança da informação, por exemplo: análise, avaliação e tratamento de risco;

III – propor e apoiar iniciativas que visem à segurança dos ativos de informação;

I. promover, junto com o Depes e o Degep, estratégia de conscientização dos colaboradores e dos parceiros em relação à relevância da segurança da informação para o negócio do CFC, por meio de campanhas, palestras, treinamentos e outros meios;

IV – analisar criticamente incidentes de segurança da informação em conjunto com o CSI;

V – manter comunicação efetiva com o CSI, com o objetivo de mantê-lo adequadamente informado sobre assuntos relacionados ao tema, que afetem ou tenham potencial para afetar o CFC;

VI – receber as denúncias sobre violações da PSI e das normas, devendo promover a tratativa das informações, a identificação do plano de ação, a mitigação de risco e o acionamento do CSI;

VIII – gerir o uso de tecnologias necessárias ao bom andamento dos negócios do CFC, incluindo ações preventivas e tratamento de incidentes com o objetivo de promover a elevação do nível de segurança da informação; e

IX – guiar ações direcionadas às questões técnicas definidas na Política de Tecnologia da Informação.

4. Departamento de Governança de TI

O Departamento de Governança de TI é responsável por:

I – monitorar, controlar e garantir que a estratégia e as diretrizes para segurança da informação, estabelecidas pelas partes interessadas, sejam cumpridas da melhor forma possível, de acordo o capital investido, ou seja, garantir que os objetivos sejam alcançados com os recursos existentes na organização;

II – disponibilizar corretamente as informações referentes à segurança da informação para as partes, que sejam do interesse delas, independentemente de obrigação legal;

III – monitorar, revisar e aprovar as diretrizes para a gestão de riscos de segurança da informação, com impacto na estratégia institucional, na imagem e nos serviços fornecidos pelo CFC;

IV – monitorar e executar a análise crítica dos controles estabelecidos considerados prioritários, com base na estratégia e na imagem institucional; e

V – solicitar, sempre que necessário, a realização de auditorias relativamente ao uso dos recursos de tecnologia da informação.

5. Recursos Humanos

O Departamento de Gestão de Pessoas (Degep) e o Departamento de Pessoal (Depes) são responsáveis por:

I – atribuir a responsabilidade quanto ao cumprimento da PSI, na fase de contratação dos colaboradores, e formalizá-la nos contratos individuais de trabalho;

II – colher as assinaturas do Termo de Responsabilidades e do Termo de Ciência da Política de Segurança da Informação dos colaboradores já contratados, bem como efetuar o arquivamento e a gestão dos documentos; e

III – comunicar à Coordenadoria de Tecnologia da Informação (CGTI), formal e prontamente, toda e qualquer alteração no quadro funcional da organização, contratações, demissões, alterações de cargos, funções, entre outros, no prazo máximo de 1 (um) dia útil, a fim de evitar acessos não autorizados e/ou desnecessários.;

6. Procuradoria Jurídica

A Procuradoria Jurídica é responsável por:

I – acompanhar e atuar, quando necessário, nos incidentes que violem significativamente a PSI e as normas de segurança da informação;

II – orientar empregados, colaboradores e a Coordenadoria de Tecnologia da Informação sobre a melhor forma de coleta e preservação de prova eletrônica, com o objetivo de manter sua eficácia para uso em juízo, quando necessário;

III – elaborar e revisar documentos jurídicos relacionados à segurança da informação;

IV – acompanhar o processo disciplinar, e validar as penalidades e exceções, quando houver;

V – revisar periodicamente e sugerir as normas de segurança da informação, de acordo com as necessidades e o perfil dos incidentes ocorridos ao longo do tempo, e sugerir adaptações da PSI; e

VI – analisar e adequar toda e qualquer regulamentação interna para que esteja em conformidade com as demais legislações pertinentes à sua área de atuação.

7. Departamento de Desenvolvimento e Integração de Aplicações

O Departamento de Desenvolvimento e Integração de Aplicações é responsável por:

I – garantir o cumprimento das regras para o desenvolvimento seguro de sistemas e softwares, de acordo com as diretrizes contidas na Política de Segurança da Informação; e

II – homologar os procedimentos e métodos aplicados no processo de desenvolvimento seguro.

8. Departamento de Suporte e Infraestrutura

O Departamento de Suporte e Infraestrutura é responsável:

I – pela gestão do uso de tecnologias necessárias ao bom andamento dos negócios do CFC, incluindo ações preventivas e tratamento de incidentes, a fim de promover maior nível de segurança da informação; e

II – pelas ações direcionadas às questões técnicas que estão definidas nas normas de tecnologia da informação.

9. Gestores

É responsabilidade de cada gestor inventariar, atribuir valor, analisar quanto aos riscos de todos os ativos de informação necessários à sua unidade organizacional.

Garantir, na sua unidade organizacional, que o descarte seja efetuado de acordo com a Tabela de Temporalidade do CFC.

Cabe aos gestores:

I – ter postura ética em relação à segurança da informação, e ser modelo de conduta para os colaboradores sob a sua gestão;

II – cumprir e fazer cumprir a Política de Segurança da Informação, as normas e os procedimentos de segurança da informação, além do Código de Conduta para os Conselheiros, Colaboradores e Funcionários dos Conselhos Federal e Regionais de Contabilidade;

III – assegurar que suas equipes possuam acesso e conheçam a Política de Segurança da Informação, as normas e os procedimentos de segurança da informação;

IV – atribuir, na fase de contratação de terceirizados e de fornecedores, quando esses necessitarem ter contato com informações do CFC, a inserção de cláusulas de responsabilidade, de ciência da Política de Segurança da Informação e de confidencialidade, e exigir da empresa contratada o repasse das obrigações aos empregados responsáveis pela prestação de serviços dentro do Conselho;

V – especificar e solicitar previamente permissão de acesso, e elencar os ativos de informação para prestadores de serviços em geral que não sejam contratados;

VI – adaptar normas, processos, procedimentos e sistemas sob sua responsabilidade para atender à Política de Segurança da Informação;

VII – comunicar imediatamente à CGTI, por meio da abertura de ticket na ferramenta de chamados (http://helpdesk.cfc.org.br/helpdesk/), eventuais violações da segurança da informação; e

VIII – garantir a devida utilização de domínios de e-mail do CFC (@cfc.org.br) pelos membros de suas equipes.

10. Colaboradores em Geral

I – cumprir, fazer cumprir e zelar, em qualquer nível hierárquico, na sua esfera de competência pela realização eficaz das normas e dos princípios da segurança da informação, de modo a manter o compromisso com os critérios legais e éticos que envolvem o CFC;

II – responsabilizar-se por qualquer prejuízo ou dano que vier a sofrer ou causar ao CFC e/ou a terceiros, em decorrência do não atendimento às diretrizes da PSI e das normas relacionadas;

III – fazer uso de senha segura, devendo essa ser alterada conforme periodicidade determinada pelo CFC;

IV – cumprir fielmente a Política de Segurança da Informação, as normas e os procedimentos de segurança da informação, além do Código de Conduta para os Conselheiros, Colaboradores e Funcionários dos Conselhos Federal e Regionais de Contabilidade;

V – buscar orientação do superior hierárquico e/ou do departamento responsável pelo Departamento de Segurança da Informação, quando houver dúvidas relacionadas à segurança da informação;

VI – assinar os termos de ciência da Política de Segurança da Informação, formalizar a ciência da Política e das normas de segurança da informação, e assumir a responsabilidade pelo seu cumprimento;

VII – proteger as informações contra o acesso, a modificação, a divulgação ou a destruição não autorizada pelo CFC;

VIII – assegurar que os recursos tecnológicos disponibilizados sejam utilizados somente para fins profissionais e de interesse do CFC.

IX – comunicar imediatamente ao Departamento de Segurança da Informação qualquer descumprimento ou violação da política, normas e procedimentos relacionados.

5. Controle de Revisões

Revisão	Item	Alteração	Data
0		Versão inicial	