CRCES
CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO

RESOLUÇÃO CRCES N.º 450, DE 15 DE DEZEMBRO DE 2022.

Institui a Política de Segurança da Informação e Privacidade no âmbito do Conselho Regional de Contabilidade do Espírito Santo - CRCES.

O **PLENÁRIO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO,** no uso de suas atribuições legais e regimentais, nos termos do inciso XVIII, art. 11, da Resolução n.º 342/2014;

CONSIDERANDO a necessária conformidade do CRCES aos termos da Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709, de 14 de agosto de 2018;

CONSIDERANDO a Portaria CRCES n.º 59, de 17 de maio de 2022, que criou o Comitê de Segurança da Informação (CSI) no âmbito do Conselho Regional de Contabilidade do Espírito Santo;

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;

R E S O L V E:

Art. 1º. Instituir a Política de Segurança da Informação e Privacidade no âmbito do Conselho Regional de Contabilidade do Espírito Santo - CRCES por meio do Manual de Segurança da Informação e Privacidade, nos termos do Anexo desta Resolução.

Art. 2º. Esta Resolução entra em vigor na data de sua assinatura.

Contadora **Carla Cristina Tasso**
Presidente

Aprovada na 1650ª Reunião Plenária, realizada em 15 de dezembro de 2022

ANEXO

MANUAL DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. INTRODUÇÃO

Com o crescimento do uso de sistema para uso na Internet cresceu proporcionalmente a preocupação com a segurança dos dados e informações que circulam por ela, fazendo-se necessárioaformulação de regras a serem seguidas.

Tanto os sistemas de informação, quanto as redes de informação das organizações, estão expostas a diversas ameaças à sua segurança, dentre elas temos: fraudes eletrônicas, espionagem, sabotagem, vandalismo, inundação, incêndio, etc. Danos causados por código malicioso, hackers também estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

É possível elevar o nível de segurança da informação por meios técnicos se apoiando em uma gestão e procedimentos apropriados. Os controles a serem implantados requerem um planejamento cuidadoso e extrema perícia e atenção.

Assim é que compete a todos os colaboradores do CRCES conhecer e fazer uso da política de segurança da informação e as normas internas de segurança da informação.

Nesse sentido, este documento tem comoobjetivo, estabelecer políticas que garantam a integridade, a confiabilidade e a transparência dos Dados e informações do Conselho Regional de Contabilidade - CRCES, definindo regras e protocolos para o uso da rede interna e externa pelos seus colaboradores a fim de se evitar o uso indevido desses dados e informações, quer seja de forma intencional ou acidental.

Esta política se aplica a todas as informações que estejam sob a responsabilidade do CRCES, em quaisquer formas ou meios e que porventura sejam apresentadas ou compartilhadas. Deverão estar sempre protegidas adequadamente, de acordo com controles definidos nesta política.

Este documento é de obrigatória utilização por todos os colaboradores, incluindo efetivos, de livre provimento e exoneração, assessores, estagiários, temporários, terceirizados, prestadores de serviço, consultores independentes ou quaisquer outros que tenham acesso a qualquer ativo de Tecnologia de Informação e Comunicação (TIC) do CRCES.

2. TERMINOLOGIA

1. Ativo: tudo que tem valor para a organização.

2. Arquivos infectados: aqueles que sofreram a ação de vírus eletrônico.

3. Caixa Postal / Correio Eletrônico: espaço em disco, onde são armazenadas as

mensagens de correio eletrônico.

4. Criptografia: ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

5. Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

6. Chave de Aceso: código de aceso atribuído a cada usuário. Para cada chave de acesso éassociada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-o acessar os recursos disponíveis.

7. *Download*: baixar um arquivo ou documento de outro computador, através da Internet.

8. Ferramenta Tecnológica: sistema (conjunto de programas) e/ou equipamento destinado a proteger, monitorar ou agregar valor aos ativos de informações.

9. *E-mail*: mensagem eletrônica.

10. Política de Segurança da Informação: documentos que provêm uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis eregulamentações relevantes.

11. *Software*: programa de computador.

12. *Spam*: qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmo a tenha solicitado.

3. COMPETÊNCIAS DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO - TI

Este setor será responsável pela gestão de todas as frentes de Segurança da Informação do CRCES e será apoiada pela Comitê de Segurança da Informação do CRCES (CSI). Sua missão é estabelecer e utilizar procedimentos para avaliar, implementar e monitorar as diretrizes de proteção da informação visando garantir a continuidade dos processos e serviços CRCES.

Compete ao Setor de TI:

I. solicitar recursos orçamentários para as ações de segurança da informação;

II. promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

III. instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

IV. coordenar e executar as ações de segurança da informação no âmbito de sua

atuação;

V. consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurançada informação;

VI. recomendar a aplicação das ações corretivas e disciplinares cabíveis nos casos deviolação da segurança da informação;

VII. credenciar e descredenciar usuários;

VIII. realizar o credenciamento mediante solicitação da chefia da área e o descredenciamento por solicitação do RH ou da chefia da área, no caso de contratos;

IX. definir os perfis de usuários cujos privilégios sejam compatíveis com as atividades do usuário;

X. instalar todos os softwares nos equipamentos do CRCES;

XI. desinstalar, sem aviso prévio, todos e quaisquer *softwares* considerados nocivos à integridade da rede e/ou sem licença de uso, em atendimento à Lei 9.609/98 (Lei do *Software*);

XII. realizar auditoria (local ou remota);

XIII. instalar softwares de monitoramento;

XIV. autorizar a conexão a redes externas.

Após a definição do perfil do usuário caberá ao chefe da área indicar os usuários que possuirão direito de leitura e/ou gravação nas pastas compartilhadas de sua área;

Os usuários não terão contas com perfil de administrador, nem contas do domínio com privilégio de administrador local da estação, exceto aqueles cuja atividade funcional necessite de tal requisito;

4. DIREITOS E DEVERES DOS USUÁRIOS

Os usuários são parte fundamental da segurança da informação deste Órgão, pois não adianta ter um nível elevado de segurança no que tange à infraestrutura e sistemas se os usuários, que são destinatários dos meios de informação, não estiverem sensíveis à necessidade de resguardar a segurança.

Compete aos usuários:

I. solicitar os serviços de TI pelo canal estabelecido por aquele Setor;

II. atualizar a versão do *software* que foi instalado pelo Setor de TI;

III. acionar e desligar os equipamentos de informática no início e término de cada expediente.

IV. encaminhar por intermédio do chefe da área os documentos de oficialização de demandas para o Setor de TI, descrevendo a necessidade e os objetivos esperados na aquisição de software e/ou hardware;

V. comunicar imediatamente ao Setor de TI sobre a existência de vulnerabilidades ou incidentes de segurança de que tenham conhecimento e que possam impactar os serviços prestados ou contratados pelo CRCES;

VI. garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.

É vedado aos usuários:

I. instalar quaisquer softwares sem prévia comunicação e autorização do Setor de TI;

II. conectar-se a redes e computadores que não os previstos pelo Setor de TI, exceto à rede *wireless* de visitantes;

III. remanejar e remover quaisquer equipamentos de informática sem aviso prévio e autorização da chefia imediata e do Setor de TI;

IV. manipular os equipamentos de rede (*switches*, *hubs*, fiação, cabeamento de rede, entre outros) sem a anuência do Setor de TI;

V. acessar ou realizar manutenção no interior do gabinete do computador, assim como trocar ou retirar componentes do mesmo, devendo ser solicitado ao Setor de TI que o faça, caso necessáro.

5. QUANTO AO USO E CRIAÇÃO DE CHAVES DE ACESSO PARA USUÁRIOS

A obrigatoriedade de observação dos procedimentos adequados para a correta utilização das chaves de acesso no ambiente de Tecnologia da Informação do CRCES será aplicada a todos os usuários que possuam chave de acesso aos sistemas, devendo ainda observarem as seguintes regras editadas pelo CRCES:

I. o *login* de rede, quando aplicado, será criado preferencialmente com o formato "*nome.sobrenome*", sendo que no caso de homonímia, utilizar-se-á "*nome. penúltimo sobrenome completo*" ou "*letras iniciais do prenome.último sobrenome completo*";

II. a identificação do empregado por senha ou outro meio é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo o usuário o responsável por guardá-la com segurança e sigilo;

III. cada sistema possui sua regra de composição de senha, entretanto, é obrigatório, desde que o sistema permita, que as senhas contenham no mínimo 12 (doze) caracteres e sejam utilizados, no mínimo, três dos tipos de caracteres abaixo:
   a) letras maiúsculas;
   b) letras minúsculas;
   c) números;
   d) caracteres especiais tais como $, %, &,@;

IV. deverá ser evitada a composição de senhas contendo somente sequência numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento e outros);

V. as senhas cadastradas terão prazo de validade de 90 (novemta) dias, ao fim do qual os usuários deverão cadastrar novas senhas.

6. QUANTO AO USO DA INTERNET

A Internet deve ser utilizada para fins de complemento às atividades do setor, para o enriquecimento intelectual de seus servidores e como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

Os empregados devem estar cientes da periculosidade da navegação na Internet, antes de acessá-la e de utilizar os seus recursos, devendo ainda cumprir os seguintes dispositivos:

I. todos os usuários ao utilizarem esse serviço deverão fazê-lo no estrito interesse do CRCES, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público;

II. o acesso à Internet por parte dos empregados utilizando equipamentos do CRCES deve ser feito exclusivamente por meio da única ligação existente entre a Internet e o Conselho, sendo vedado o acesso à Internet utilizando provedores de acesso privados para o acesso à rede mundialde computadores;

III. é expressamente proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;

IV. a infraestrutura do CRCES e os recursos de informática jamais devem ser utilizados para a realização de trabalhos de terceiros ou de atividades paralelas.

7. QUANTO À UTILIZAÇÃO DO CORREIO ELETRÔNICO

Os *e-mails* são uma excelente forma de comunicação, porém são fonte de vulnerabilidade para as informações organizacionais, razão pela qual deverão ser aplicadas aos ativos de informação e comunicação do CRCES a seguintes regras:

I. os *e-mails* corporativos serão criados preferencialmente no formato: função@crc-es.org.br ou nome.sobrenome@crc-es.org.br;

II. o acesso às mensagens de correio eletrônico são de exclusividade do empregado detentor do endereço eletrônico, sendo garantida a inviolabilidade do conteúdo das mensagens eletrônicas, entretanto, todas as mensagens podem ser monitoradas e são passíveis de auditoria;

III. as auditorias poderão ser solicitadas, a qualquer momento, pela Diretoria do CRCES e realizadas pelo Setor de TI;

IV. os e-*mails* departamentais compartilhados serão criados quando solicitado pelo gestor da área e podem ser acessados por vários empregados;

V. os *e-mails* do CRCES devem ser utilizados apenas para assuntos referentes ao Conselho sendo vedado reenvio de mensagens que não estejam diretamente ligadas ao Órgão;

VI. é vedado o uso de *e-mail* para propaganda política, racial, financeira ou de qualquer outra natureza;

VII. é vedado o uso de material pornográfico entre os *e-mails* da organização, tanto recebimento como envio;

VIII. é expressamente proibida a abertura de Anexos com as extensões **.**bat, **.**exe, **.**src, **.**lnk e **.**com, sem o conhecimento prévio doSetor de TI, ou de quaisquer outros formatos por este alertado;

IX. deve-se evitar enviar anexos com tamanho superior a 15MB.

8. QUANTO AO ARMAZENAMENTO DE ARQUIVOS

Trata-se da regras e requisitos básicos aplicadas aos ativos de informação para armazenamento de arquivos no Setor de Tecnologia da Informação do CRCES.
Os arquivos da rede do CRCES estão disponibilizados em unidades mapeadas na própria máquina do usuário, da maneira que se segue:

I. Servidor de arquivos: é um serviço disponibilizado pelo Departamento de TI para os funcionários acessarem utilizando *login* e senha da rede gerenciada pelo *active directory* do CRCES. É uma área do disco rígido de um dos servidores que disponibiliza para os usuários as pastas e documentos relativos ao setor onde trabalha.

II. Serviço de Cópias de Sombra de Volume: trata-se de uma rotina que possibilita criar uma cópia de sombra consistente (também conhecida como um instantâneo ou uma cópia pontual) dentro das pastas mapeadas, possibilitando restaurar arquivos ou pastas inteiras em caso de perda acidental ou alteração indevida.

III. *Backup*: refere-se a uma cópia de segurança diária dos arquivos de banco de dados do sistema gestor, possibilitando ao gestor de Tecnologia da Informação a recuperação dos mesmos em caso de perda acidental e/ou forçada.

IV. Replicação de dados em nuvem: o CRCES replica uma fração da massa de dados do sistema gestor para uma aplicação na nuvem, esse compartilhamento torna possível disponibilizar ao profissional da Contabilidade os "serviços online".

V. *Backup* de dados em nuvem: os dados replicados para a aplicação em nuvem geram um *backup* em ambiente segregado, na própria nuvem onde está hospedada a massa de dados do serviço. O armazenamento na nuvem é um modelo de computação que armazena dados na Internet por meio de um provedor de computação que gerência e opera o armazenamento físico de dados. É importante ressaltar que no armazenamento em nuvem é de responsabilidade do usuário realizar *backup* e controlar o acesso aos dados.

9. PENALIDADES

Técnicos do Setor de TI identificarão os usuários que descumprirem qualquer item deste Manual de segurança da informação.

As penalidades serão aplicadas observando o seguinte:

I. o usuário que apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, arquivo ou programa de computador, de forma indevida ou não autorizada, fizer uso indevido dos equipamentos de informática, bem como praticar ato em desacordo com os termos da presente norma fica sujeito às punições cabíveis nos termos da lei.

II. o usuário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu chefe imediato e a Diretoria do CRCES.

III. todos os usuários ao tomarem conhecimento de qualquer incidente de segurança da informação, devem informar o ocorrido, imediatamente, à administração.

IV. na primeira transgressão o empregado será notificado, sobre o item que transgrediu e orientado para não mais infringir, sob pena de sofrer outras sanções.

V. na segunda transgressão o empregado será notificado novamente, mais com cópia para chefia imediata, do descumprimento das normas estabelecidas neste documento. Caso na infração cometida esteja caracterizando qualquer tipo de crime (acesso a *sites* de pedofilia, racismo, etc.), tomar-se-ão providências

previstas em lei.

VI. O usuário arcará pelos danos causados pelo mau uso dos computadores e dos recursos do CRCES, mediante apuração cabível, nos termos da lei.

10. DISPOSIÇÕES FINAIS

O CRCES se reserva no direito de monitorar o tráfego através das suas redes de comunicação, incluindo o acesso à Internet.

O CRCES se reserva no direito de verificar, sempre que julgar necessário, a obediência às normas ou procedimentos citados neste documento.

O uso indevido dos serviços de correio eletrônico, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente.

Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente norma.

Todos os equipamentos do CRCES devem ser mantidos em boas condições e possuir proteção de forma a preservar seus componentes internos.

A saída de equipamentos do CRCES deve ser registrada utilizando documento de saídade equipamento assinada pelo superior imediato.

11. REFERÊNCIAS LEGAIS

1. Lei Federal n.º 8.159, de 08 de janeiro de 1991, que dispõem sobre a Política Nacional de Arquivos Públicos e Privados.

2. Lei Federal n.º 10.406, de 10 de janeiro de 2002 – Código Civil.

3. Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados-LGPD.

4. Decreto Federal n.º 4.453, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal.

5. Decreto n.° 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação.

6. Norma ABNT/NBR ISO 27.701/2019.