CRCSC
CONSELHO REGIONAL DE CONTABILIDADE DE SANTA CATARINA

RESOLUÇÃO CRCSC N.º 454, DE 08 DE MARÇO DE 2022.

Aprova o Plano Diretor de Tecnologia da Informação (PDTI) do Conselho Regional de Contabilidade de Santa Catarina, biênio 2022/2023.

O **CONSELHO REGIONAL DE CONTABILIDADE DE SANTA CATARINA,** no uso de suas atribuições legais e regimentais,

Considerando as recomendações do Tribunal de Contas da União acerca da necessidade de elaboração de um Plano Diretor de Tecnologia da Informação (PDTI), contemplando as ações associadas às metas da entidade, antes de executarem gastos relacionados à Tecnologia da Informação;

Considerando que o Plano Diretor de Tecnologia da Informação (PDTI) é um documento de planejamento das ações de TI que apoiam as atividades finais da entidade;

Considerando a Instrução Normativa n.º 1, de 4 de abril de 2019, da Secretaria de Logística e Tecnologia da Informação do Planejamento, que dispõe sobre o processo de contratação de soluções de tecnologia da informação e determina que as contratações de TI devem ser precedidas de planejamento, elaborado em harmonia com o PDTI;

Considerando a proposta encaminhada pelo Comitê de Tecnologia da Segurança da Informação (CTSI) deste Conselho,

R E S O L V E:

Art. 1º Aprovar o Plano Diretor de Tecnologia da Informação (PDTI) do Conselho Regional de Contabilidade de Santa Catarina, referente ao biênio 2022/2023, disponível no sítio www.crcsc.org.br.

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

Contadora **Marisa Luciana Schavabe de Morais**
Presidente

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO – PDTI

Departamento de Tecnologia da Informação

dezembro de 2021 | Versão 1.2

Histórico de Versões

Data	Versão	Descrição	Autor
13/10/2021	0.9	Esboço	Fernando Proenço Zucatto
02/12/2021	1.0	Primeira Entrega	Fernando Proenço Zucatto
02/12/2021	1.1	Término da Metodologia	Fernando Proenço Zucatto
02/12/2021	1.2	Finalização do Cronograma -Divisão de Tarefas -Matriz de Conhecimento	Fernando Proenço Zucatto

Índice

1 INTRODUÇÃO

O Plano Diretor de Tecnologia de Informação Biênio 2022-2023, criado pelo Departamento de Tecnologia de Informação, planeja e orienta as ações do Conselho Regional de Contabilidade, sempre em alinhamento com o Orçamento Anual e as diretrizes institucionais do Conselho Regional de Contabilidade de Santa Catarina (CRCSC).

2 VISÃO GERAL

2.1. Objetivo

Planejar e orientar ações do âmbito da Tecnologia da Informação, visando melhor atendimento aos usuários, sejam internos ou externos, assim como a proteção dos dados do Conselho. Tem como abrangência os anos de 2022 e 2023, sendo que deverá ser revisto trimestralmente, para acompanhamento do cronograma e correções devidas conforme demanda institucional.

2.2. Justificativa

A elaboração de um Plano Diretor de Tecnologia de Informação se faz necessária para que haja um documento formal, aprovado em Conselho Diretor e Plenária do CRCSC, sobre as ações que serão realizadas nos anos subsequentes, realizando assim um planejamento de curto e médio prazo.

2.3. Contexto da Unidade de TI

2.3.1 Equipe

A formação e atividades da equipe de TI do CRCSC, por alinhamento da gestão na última década, tem sido a nível de suporte ao usuário. Sendo contratada empresa de consultoria para nível avançado das demandas. Com isso, o CRCSC consegue manter uma equipe mais enxuta, ganha em economicidade, reduz gastos em treinamentos complexos e consegue manter suporte adequado aos usuários internos e externos.

A equipe de TI é composta por um coordenador, um técnico em informática, um assistente de suporte em informática e um estagiário, são eles:

Nome	Cargo	Divisão de Trabalho*
Fernando Proença Zucatto	Coordenador de Comunicação e Tecnologia da Informação	Gestão, Novos Projetos, PDTI, DFDs, *Compliance*, Riscos e Office 365.
Fernando Proença Zucatto	Coordenador de Comunicação e Tecnologia da Informação	SPW, Rede, WiFi, Backup e Telefonia.
Fernando Vill	Assistente de Suporte em Informática	Office 365, Rede, Wifi, Hardware, Suporte as Delegacias Regionais.
Luiz Arthur Dutra Lentz	Estagiário de Informática	Suporte ao Usuário Interno.

A divisão de trabalho apenas mostra a prioridade de atendimento de cada demanda por empregado, entretanto, todos deverão estar capacitados e darão o suporte necessário para todas as atividades inerentes ao setor de Tecnologia da Informação.

Diante deste quadro atual e para manter a qualidade dos serviços que uma TI deve oferecer a todos os seus usuários, o CRCSC, por meio de processo licitatório conforme determina a Lei nº 8.666/93, tem como contratada, uma empresa de tecnologia, TECJUMP Tecnologia em Informática Ltda, para prestar serviços de TI, relacionado com infraestrutura de servidores, segurança de rede, comunicação de dados, comunicação telefônica VoIP, interconexão de redes, firewall, wifi, backup, serviços de hospedagem de site e e-mails, consultoria e suporte técnico em nível de hardware e software para o CRCSC.

2.3.2 Hardware

A tabela abaixo detalha os equipamentos em uso até dezembro de 2021:

Hardware	Data de Aquisição	Quantidade
Desktop (Workstation HPZ240)	2019	3
Desktop (HP Elitedesk 800 G2 SFF)	2017	24
Desktop HP (Core-i5)	2013	6
Desktop HP (Core-i5)	2012	12
Desktop HP (Core-i5)	2011	06
Desktop (Core-i5)	2010	23
Desktop (Core2Duo)	2009	08
Desktop (Celeron)	2006	01
Notebook (Vaio FE14)	2020	17
Notebook (Dell Vostro 3481)	2019	12
Notebook (Inspiron 15 7572)	2018	01
Notebook (Ultrabook Core-i5)	2015	17
Notebook (Core-i5)	2012	08
Notebook (Core2Duo)	2009	10
Notebook (Celeron)	2004	01
Monitores (HP 24“)	2019	45
Tablet (IPDA2)	2012	02
Workstation (HP Z2 G4)	2019	3
Servidor Dell (R640)	2017	2
Servidor (Arquitetura Desktop)	2009	1
Scanner	2020	7

Scanner	2017	1
Scanner	2012	4
Scanner	2009	1
Scanner	2007	1
Projetor	2016	6
Projetor	2010	4
Projetor	2008	1
Projetor	2005	1

2.3.3 Software

A tabela abaixo detalha os sistemas em uso até dezembro de 2021:

Software Licenciados	Área de Negócio	Quantidade de Licenças
Microsoft Basic Business	Informática	74 (setenta e quatro)
Microsoft 365 Apps for Business	Informática	66 (sessenta e seis)
Microsoft Power BI Pro	Informática	4 (quatro)
TeamViewer Licença Corporate	Informática	1 (uma)
Windows Server	Informática	4 (quatro)
Adobe Creative Cloud	Comunicação	3 (três)
Adobe Premiere Pro	Comunicação	1 (uma)
Corel Draw	Comunicação	4 (quatro)
CP-Pro	Jurídico	8 (oito)
Prodimage (banco de Imagem)	Relacionamento	2 (duas)
Sênior Folha de pagamento	Recursos Humano	1 (uma)
Dimep (Cartão Ponto)	Recursos Humano	1 (uma)
Sistema Geren. De Atendimento (SGA)	Relacionamento	1 (uma)
Antivírus Kaspersky	Informática	100 (cem)
Sistema Spiderware - SPW (ERP)	Informática	1 (uma)
Windows 10 OEM	Informática	100 (cem)
Windows 7 OEM	Informática	14 (catorze)
Office Home and Business 2016 Microsoft	Informática	24 (vinte quatro)
MS Office SmallBusiness 2010 FPP	Informática	23 (vinte e três)
MS Office SmallBusiness 2007 OEM	Informática	33 (trinta e três)

MS Office Professional 2007 OEM	Informática	11 (onze)
IOS OEM	Informática	2 (dois)
SQLServer 2012	Informática	2 (duas)

2.4. Alinhamento Estratégico

O CRCSC segue o planejamento estratégico do Sistema CFC/CRCs, que foi instituído pela Deliberação CFC nº 57/2018, conforme abaixo:

- **Missão do Sistema CFC/CRCs:** Inovar para o desenvolvimento da profissão contábil e zelar pela ética e qualidade na prestação dos serviços, atuando com transparência na proteção do interesse público.
- **Visão do Sistema CFC/CRCs:** Ser reconhecido como uma entidade profissional partícipe no desenvolvimento sustentável do País e que contribui para o pleno exercício da profissão contábil no interesse público.
- **Valores do Sistema CFC/CRCs:** Ética; Excelência; Confiabilidade; e Transparência.

Cabe também ressaltar que no Mapa Estratégico do Sistema CFC/CRCs, a orientação para Resultado Econômico é "garantir sustentabilidade orçamentária financeira do Sistema CFC/CRCs".

2.5. Fatores Motivacionais

Atender orientação do Conselho Federal de Contabilidade (CFC), legislação vigente e dar transparência, publicidade, assim como realizar planejamento de ações para que possam ser acompanhadas pelos gestores do CRCSC.

2.6. Premissas e Restrições

- Tornar o processo de implantação do PDTI um compromisso institucional do Conselho Diretor, Diretoria Executiva, dos gestores e dos empregados do CRCSC;
- Compor um quadro de competências de TI com as especialidades necessárias para atender às ações e aos projetos definidos no PDTI;
- Garantir recursos humanos, orçamentários e financeiros para a execução das ações e dos projetos do PDTI;
- Difundir o modelo de governança e gestão de riscos de TI para o CRCSC;
- Implantar a estrutura organizacional de TI proposta neste documento;
- Descrever o processo conceitual referente às necessidades de informação, antes de iniciar sua automação;
- Atender o plano de trabalho e orçamento do CRCSC estipulado;
- Capacitação de empregados;
- Retenção de talentos - a ser implantado com o Plano Anual de Treinamentos.

3 COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO (CTSI)

Nome	Cargo
José Mateus Hoffmann	Coordenador do Comitê e VP de Desenvolvimento Profissional
Marcelo Machado de Freitas	Conselheiro do CRCSC
Cleber Dias	Diretor de Administração e Infraestrutura
Marilúcia Etelvina Dias	Coordenadora Depto. Fiscalização, Ética e Disciplina
Alexandra Somer Bernardes	Coordenadora Depto. Registro e Relacionamento
Ricardo Minatto Tonetto	Coordenador Depto. Desenvolvimento Profissional
Leandro Pinheiro	Assessor de Projetos
Fernando Proenço Zucatto	Coordenador Depto. De Tecnologia da Informação
Fernando Vill	Assistente de Suporte de Informática

4 PARTES INTERESSADAS

- Conselho Diretor;
- Conselheiros;
- Diretorias;
- Departamentos;
- Sociedade;
- Profissionais da Contabilidade.

5 METODOLOGIA APLICADA

A metodologia escolhida foi a estabelecida pelo Ministério da Economia - Planejamento, Desenvolvimento e Gestão – www.planejamento.gov.br

Quanto a decisão de princípios e diretrizes, foi feita análise da Matriz SWOT, que se refere a um conjunto de quatro palavras: *"Strengths", "Weaknesses", "Opportunities"* e *"Threats"*, em português, FOFA - Forças, Oportunidades, Fraquezas e Ameaças.

A Matriz SWOT avalia a empresa olhando para suas forças e fraquezas, também levando em consideração os fatores internos e externos a organização.

- **FORÇAS**
  - Parque tecnológico atualizado;
  - Rápido atendimento da empresa terceirizada de consultoria em ampla variedade de suporte;
  - Grandes investimentos realizados nos biênios de 2016-2017, 2018-2019 e 2020-2021 em hardware e software;

- Contratação de novos links de internet com o dobro de capacidade, aumentando fluidez nos serviços e adequando a nova realidade de trabalho híbrido durante a pandemia;
- Contratação de terceirizado para apoio na implementação de políticas da Lei Geral de Proteção de Dados LGPD, com foco nas premissas e diretrizes de segurança digital do CRCSC.

- **FRAQUEZAS**

  Falta de integração dos sistemas;

  - Ausência de plano de governança e *compliance*;
  - Pouco mapeamentos de processos e controles;
  - Sistema de ERP defasado, muitos dados, poucas informações;
  - Orçamento limitado para o próximo biênio;
  - Equipe técnica interna sem habilidade na área de programação.

- **OPORTUNIDADES**
  - Aprovação do Plano de *Compliance* do CRCSC;
  - Altos investimentos em hardware e software no passado, foco em processos;
  - Novas perspectivas com solução de Business *Intellingence*;
  - Oferta de capacitação para os empregados já mapeada nos Orçamentos 2021 e 2022;
  - Implantação de Business *Intelligence*;

- **AMEAÇAS**
  - Possível aprovação da PEC 108/2019 – possibilidade de redução drástica do orçamento;
  - Mudança de gestão para o próximo ano poderá acarretar alteração de prioridades;
  - Novas legislações frequentes na área de segurança e proteção de dados.

6 PRINCÍPIOS E DIRETRIZES

No final dos anos de 2020 e 2021, o CRCSC realizou uma suplementações em seu orçamento para renovação de seu parque tecnológico, tendo em vista um orçamento enxuto para os próximos dois anos na área de tecnologia, atendendo a orientação para Resultado Econômico já descrita neste documento. Desta forma, para o biênio 2022-2023 temos como princípio a economicidade e nossa diretriz será investir em segurança e proteção de dados e informações, atendendo às premissas da Lei Geral de Proteção de Dados (LGPD).

7 DOCUMENTOS DE REFERÊNCIA

- Modelo de Referência do Ministério da Economia - Planejamento, Desenvolvimento e Gestão;

- Plano Diretor de Tecnologia de Informação Biênio 2020-2021;
- Proposta Orçamentária e Plano de Trabalho do CRCSC de 2022;
- Portaria CRCSC nº 059/2017 Cria o Comitê de Tecnologia e Informação do CRCSC;
- Portaria CRCSC nº 075/2021 Institui o Comitê de Tecnologia e Segurança da Informação.

8 SEGURANÇA

O aumento de ataques cibernéticos nos últimos anos faz com que o CRCSC deva estar cada vez mais preocupado com a segurança das informações e de seus sistemas.

Com a Lei Geral de Proteção de Dados (LGPD) vigorando desde agosto de 2020, as empresas precisam ficar ainda mais atentas à segurança. Afinal, elas serão responsabilizadas pela proteção e tratamento correto dos dados dos clientes que estiverem sob sua custódia.

8.1. Antivírus e Firewall

O CRCSC possui 100 (cem) licenças do Kaspersky Antivírus, quantidade suficiente para todos as estações de trabalho e servidores. O Kaspersky há mais de 20 anos é reconhecido como especialistas no combate ao malware e ao crime cibernético. Em 2018, os produtos da Kaspersky participaram de 88 testes e análises independentes, ocupando 73 primeiros lugares e ficando 77 vezes entre as três primeiras posições. Sendo reconhecido como líder global em cibersegurança. Cabe ressaltar que todos os computadores e notebooks ao serem cadastrados na rede do CRCSC, são configurados para fazerem automaticamente todas as atualizações do antivírus, sendo que o usuário não pode cancelar o procedimento e nem fechar o aplicativo de antivírus.

Em 2019 o CRCSC elevou sua proteção a um novo patamar ao adquirir novo firewall Sophos XG135 Appliance, saindo de um firewall software e passando para camada de hardware. A solução de firewall UTM Sophos é uma das líderes de mercado segundo o quadrante mágico do Garther, pelo quinto ano consecutivo, assim como foi a solução vencedora em testes realizados pela Miercom.

Importante salientar que todos os dispositivos conectados na rede do CRCSC são reconhecidos pelo firewall e só conseguem acessar a *world wide web* caso configurados para tal.

8.2. Política de Segurança da Informação

O CRCSC sabe que a informação é um de seus mais importantes ativos e que, diante dos diversos meios de acesso a serviços, banco de dados, e-mails e redes de dados, ela se torna alvo de constantes ameaças internas e externas e que, quando não gerenciadas adequadamente, essas ameaças podem causar danos consideráveis a uma organização.

Sendo assim, surge a necessidade de formalizar e estabelecer regras e padrões para proteção da informação, definindo diretrizes e regras a serem seguidas para a implantação e manutenção de uma Política de Segurança da Informação do CRCSC. Sendo aprovada e publicada pela Portaria CRCSC XXX/XXXX. Tal documento encontra-se como anexo deste PDTI.

8.3. Backup e Espelhamento de Servidores

O Departamento de Tecnologia da Informação do CRCSC tem a ciência de que mesmo com

as melhores soluções no mercado de segurança, não é garantido a total imunidade a invasões. Desta forma, foram instauradas diversas rotinas de backup, evitando assim que haja perda das informações, são elas:

8.3.1 Backup Físico Semanal

Sistema de quatro HDs externos de backup, que são trocados semanalmente e contam com todos os arquivos, VMs, bancos de dados, enfim, a totalidade das informações armazenadas no CRCSC. São aplicados alternadamente, enquanto um está realizando a rotina de backup, os outros estão armazenados em local seguro fora do CRCSC, evitando assim que um desastre na sede do CRCSC destruísse todas as informações.

8.3.2 Backup Físico Diário Banco SQL

Diariamente é realizado, em um HD externo, backup dos bancos de dados do sistema ERP do CRCSC, hoje SPW. Desta forma, em um incidente menos grave, seria possível recuperar informações D-1.

8.3.3 Espelhamento de Servidores

O CRCSC conta com dois servidores que replicam suas informações a todo o tempo. Sendo assim, caso haja a indisponibilidade de um dos servidores, os serviços continuaram funcionando sem interrupção.

8.3.4 Backup em Nuvem Azure

A todo momento é realizado backup da totalidade das informações do CRCSC em nuvem, na plataforma Azure da Microsoft. Funcionando como um plano C, caso todas as opções anteriores venham a falhar.

9 LINKS DE INTERNET

Em 2019 o CRCSC passou a contar com 2 (dois) links dedicados de 100mb, contratados de empresas diferentes, para acesso à internet. Os links funcionam de forma redundante, desta forma não há indisponibilidade dos serviços.

10 PLANEJAMENTO DO ORÇAMENTO

#	Projeto	Descrição	Previsão Orçamentária	Ações
1	5002	Tecnologia da Informação	15.000,00	SERVIÇO DE ASSESSORIA E CONSULTORIA
2	5002	Tecnologia da Informação	469.078,39	SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO
3	5002	Tecnologia da Informação	3.700,00	ASSINATURAS

16	5010*	Modernização do Parque de Informática	92.000,00	EQUIPAMENTOS DE PROCESSAMENTO DE DADOS
17	5010	Modernização do Parque de Informática	95.359,81	Contratação de software de controle de processos

11 CRONOGRAMA DE AÇÕES 2022

#	Atividade	1º Quadrimestre	2º Quadrimestre	3º Quadrimestre	Responsável	Situação
1	Contratação de 03 licenças Adobe Pro	x			Departamento Jurídico	Programado
2	Renovação de Licenças Power BI PRO			x	Departamento de TI	Programado
3	Renovação de Licenças Office 365			x	Departamento de TI	Programado
4	Contratação de serviços terceirizados de suporte de rede e servidores, e fornecimento de solução de backup, firewall e wifi.		x		Departamento de TI	Programado
5	Contratação de serviços eventuais de manutenção em delegacias regionais	x	x	x	Departamento de TI	Demanda
6	Renovação de 05 licenças Adobe Pro		x		Departamento Fiscalização	Programado
7	Renovação locação de impressoras multifuncionais			x	Departamento de TI	Programado
8	Renovação dos dois links de internet 100 mb		x		Departamento de TI	Programado
9	Renovação locação central telefônica	x			Departamento de TI	Programado
10	Renovação link telefonia sede	x			Departamento de TI	Programado
11	Renovação Sistema de Gestão Integrada - SPW			x	Departamento de TI	Programado
12	Renovação Link de internet Delegacias Regionais	x	x	x	Departamento de TI	Demanda
13	Aquisição de 11 notebooks para os Fiscais		x		Departamento de TI	Programado
14	Aquisição 15 suporte para apoio notebook		x		Departamento de TI	Programado
15	Dotação extra para eventuais contratações	x	x	x	Departamento de TI	Demanda

16	Renovação de sistema de suporte remoto			x	Departamento de TI	Programado
17	Aquisição 20 adaptadores USB-C para VGA		x		Departamento de TI	Programado
18	Aquisição 12 HD´s SSD upgrade Notebooks Dell		x		Departamento de TI	Programado
19	Aquisição 10 HDs SSD Reserva Técnica		x		Departamento de TI	Programado
20	Aquisição 30 Kits Mouse e Teclado sem fio Reserva Técnica		x		Departamento de TI	Programado
21	Revisar PDTI trimestralmente	x	x	x	Comitê PDTI	Programado
22	Capacitar equipe para módulos do SPW			x	Departamento de TI	Programado
23	Capacitação interna em Office 365 Essentials		x		Departamento de TI	Programado
24	Capacitação interna equipe nas tarefas operacionais como: impressoras, firewall, backup, telefonia, wifi e outras atividades rotineiras		x	x	Departamento de TI	Programado
25	Divulgar política de segurança da Informação e proteção de dados no CRCSC	x	x	x	Departamento de TI	Programado
26	Manutenção de hardware e sistemas	x	x	x	Departamento de TI	Demanda
27	Aquisição de 20 Head sets Reserva Técnica		x		Departamento de TI	Programado
28	Capacitação Interna para utilização de sistema de *Business Intelligence(BI)*	x	x	x	Departamento de TI	Programado
29	Aquisição equipamento Jabra para otimizar áudio em reuniões com até 06 pessoas.		x		Departamento de TI	Programado
30	Mapeamento processos setor de TI	x	x	x	Departamento de TI	Programado
31	Aquisição servidor de arquivos NAS		x		Departamento de Comunicação	Programado
32	Locação sistema de câmeras/monitoramento prédio Sede	x			Departamento de TI	Programado
33	Renovação licenças antivírus parque TI			x	Departamento de TI	Programado
34	Renovação consultoria *Business Intelligence(BI)*	x			Departamento de TI	Programado
35	Renovação serviços de telefonia móvel			x	Departamento de TI	Programado

12 PLANEJAMENTO DE AÇÕES 2022

#	Atividade	1º Quadrimestre	2º Quadrimestre	3º Quadrimestre	Responsável	Situação
1	Upgrade SSDs e Windows 10 máquinas delegacias regionais	x			Departamento de TI	Programado
2	Contratação de sistema de gerenciamento de suporte	x			Departamento de TI	Programado
3	Aquisição de 15 notebooks	x			Departamento de TI	Programado
4	Aquisição de 20 mouse/teclado sem fio	x			Departamento de TI	Programado
5	Aquisição de 20 fones de ouvido c/ microfone	x			Departamento de TI	Programado
6	Aquisição de notebook de alta performance para BI	x			Departamento de TI	Programado
7	Capacitação para utilização de sistema de *Business Intelligence*	x	x	x	Departamento de TI	Programado
8	Integrar sistema de telefonia com banco de dados SQL utilizado pelo SPW		x		Departamento de TI	Programado
9	Mapeamento processos		x		Departamento de TI	Programado
10	Matriz de conhecimento		x		Departamento de TI	Programado
11	Definir e implantar processos de governança e gestão de riscos de TI no CRCSC		x	x	Departamento de Governança e TI	Programado
12	Capacitação interna em Office 365 Essentials			x	Departamento de TI	Programado
13	Capacitação para Gestão de Riscos e Governança			x	Departamento de TI	Programado
14	Capacitação interna equipe na gestão da rede, VPN e firewall do CRCSC			x	Departamento de TI	Programado
15	Capacitação interna equipe nas tarefas operacionais como: impressoras, backup, telefonia, wifi e outras atividades rotineiras			x	Departamento de TI	Programado

13 REALIZAÇÕES DOS ANOS ANTERIORES

2020-2021
Revisão de Política de Segurança da Informação
Aquisição de 17 notebooks
Aquisição de webcams e alto falantes bluetooth para webconferências
Implantação de novas rotinas de backup
Aquisição de sistema de suporte remoto
Renovação com empresa de suporte especializada, aumentando escopo de serviços
Renovação de sistema de webconferências
Aumento de licenças da suíte de aplicativos Office 365 para todos os empregados e estagiários
Aumento de licença do Adobe Creative Cloud
Segmentação de rede em VLANs aumentando a segurança
Troca antenas Wifi melhorando qualidade de sinal e alcance
Integração Sistema SPW x Plataforma EAD
Integração base de dados CRCSC x SEFAZ
Substituição carimbos protocolo por etiquetas impressas SPW com informação do processo
Ativação notificações módulo Protocolo SPW
Implantação Requerimentos WEB aos profissionais pelos serviços on-line
Upgrade HDs SSD e Memória nas máquinas Desktop
Troca máquinas Desktop das Delegacias
Migração de E-mails e DNS da Revista CRCSC
Troca banco de baterias Nobreak da Sala dos Servidores TI
Implantação aplicativo Wiipo para visualização de holerite
Renovação com dobro da velocidade links de internet
Atualização base de CEPs no sistema SPW
Migração imagens antigas PRODimage para sistema SPW
Renovado registro do domínio *.crcsc.org.br por 10 anos
Criado controle de quantidade de atendimentos de suporte TI
Padronização de E-mails dos setores
Disponibilizado módulo de Documentos sem Fase para assinatura de ATAs pelo Portal de Assinaturas
Criados 06 Painéis BI para setor de Fiscalização
Criados 06 Painéis BI para setor de Registro
Implantado Sistema de Diárias pelo SPW

Implantada Integração de pagamentos SPW x CEF
Criada estrutura Reuniões Híbridas

O Plano Diretor de Tecnologia da Informação Biênio 2020-2021 teve grande importância nos avanços do Departamento de Tecnologia da Informação. Conforme demonstrado acima, toda a parte de segurança foi revista, assim como aquisições de hardwares e licenças de suítes profissionais de aplicativos de escritório para todos os usuários.

Cabe ressaltar também, uma mudança de estratégia, buscando uma mobilidade dos usuários, com a aquisição de licenças para acesso remoto, notebooks, sistema de webconferências, comunicação interna e computação em nuvem. Entretanto, não houve avanços quanto a mapeamento de processo e gestão de riscos, essas ficaram para o próximo biênio, setor de Governança e consultoria de implantação da Lei Geral de Proteção de Dados auxiliarão os departamentos nesse processo.

2018-2019
Implantação de Política de Segurança da Informação
Contratação de sistema de comunicação interna
Implantação de novo serviço de firewall
Implantação de novo sistema de gerenciamento do Wifi
Contratação de novos links dedicados de internet
Aquisição de 15 notebooks
Aquisição de webcams e alto falantes bluetooth para webconferências
Modernização do sistema de som do plenário do CRCSC
Contratação de sistema de armazenamento em nuvem
Contratação e novo servidor de correio eletrônico
Implantação de novas rotinas de backup
Aquisição de sistema de suporte remoto
Contratação de empresa de suporte especializada, aumentando escopo de serviços
Aquisição de 3 workstations
Aquisição de 45 monitores de 24”
Contratação de sistema de webconferências
Aquisição de licenças da suíte de aplicativos Office 365 para todos os empregados e estagiários
Aumento de licença do Adobe Creative Cloud
Aumento de licença do Adobe Stock
Sistema em nuvem de prestação de contas das delegacias de representação

2016-2017
Aquisição de 24 desktops
Aquisição de 24 licenças Office 2016
Aquisição de 2 novos servidores
Aquisição de 100 licenças profissionais de antivírus
Reestruturação de todo cabeamento de rede do CRCSC
Aumento de licença do Adobe Creative Cloud

O Plano Diretor de Tecnologia da Informação Biênio 2016-2017 foi o primeiro feito pelo Conselho Regional de Contabilidade de Santa Catarina. Apesar de um pouco restrito, devido pouca familiaridade com o assunto, foi importante para criar a cultura de documentação e planejamento no Departamento de TI, e teve grande avança ao que diz a infraestrutura, pois foi realizado grande projeto de reestruturação de cabeamento e aquisição de novos servidores.

14 PLANEJAMENTO REUNIÕES DO COMITÊ PDTI

2022	1º Trimestre	2º Trimestre	3º Trimestre	4º Trimestre	Situação
1. Planejamento anual	x				Programada
2. Primeira revisão		x			Programada
3. Segunda revisão e planejamento próximo ano			x		Programada
4. Revisão anual				x	Programada

2023	1º Trimestre	2º Trimestre	3º Trimestre	4º Trimestre	Situação
5. Planejamento anual	x				Programada
6. Primeira revisão		x			Programada
7. Segunda revisão e planejamento próximo biênio			x		Programada
8. Revisão anual				x	Programada

ANEXO I

CRCSC
CONSELHO REGIONAL DE CONTABILIDADE
DE SANTA CATARINA

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Política de Segurança da Informação

dezembro/2021

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CRCSC

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Seção I
DAS PREMISSAS

Art. 1º Proteger os dados pessoais, a privacidade e o acesso à informação, valorizando o princípio da autodeterminação informativa, mas também o direito à informação, o legítimo interesse, a liberdade de expressão, o direito à opinião, a inviolabilidade da intimidade, da honra e da imagem dos titulares de dados pessoais, o desenvolvimento tecnológico e a inovação, a livre iniciativa, os direitos do consumidor, o livre desenvolvimento da personalidade e a cidadania;

Art. 2º Proteger a informação institucional e de cadastros, visando minimizar danos às finalidades institucionais, prevenir fraudes e maximizar o retorno dos investimentos e oportunidades, de acordo com a sua sensibilidade e exposição ao risco;

Art. 3º Garantir condições para que os empregados, estagiários, prestadores de serviços, conselheiros e, quando aplicável, terceiros e quaisquer outras pessoas que prestem serviços ao CRCSC sejam orientados sobre a existência e a utilização dos instrumentos normativos, dos procedimentos e dos controles de segurança adotados pelo CRCSC.

Seção II
DOS OBJETIVOS

Art. 4º A Política de Segurança da Informação (PSI) tem por finalidade estabelecer normas, diretrizes e procedimentos para a segurança no uso, tratamento e controle, proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio de informação e comunicação, de forma a garantir a disponibilidade, integridade e confidencialidade das informações no âmbito do Conselho Regional de Contabilidade de Santa Catarina.

Parágrafo único. A PSI está alinhada às estratégias instituticionais, com a política de governança, com a gestão de riscos e com os normativos que regem a matéria.

Art. 5º A PSI trata do uso e do compartilhamento de dados, informações e documentos no âmbito do CRCSC, em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), objetivando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação.

Art. 6º Para a segurança da informação no CRCSC, serão rigorosamente observados o compromisso institucional com a proteção das informações de sua propriedade e/ou sob sua guarda, a participação e o cumprimento por todos os colaboradores em todo o processo

e o disposto neste normativo, nas disposições constitucionais, legais e regimentais vigentes.

Seção III
DOS PRINCÍPIOS BÁSICOS

Art. 7º A PSI do CRCSC orienta-se pelos seguintes princípios básicos:

I – Disponibilidade: garante que a informação esteja sempre acessível para uso legítimo de pessoas físicas, sistemas e entidades autorizadas;

II – Integridade: garante que a informação esteja correta, confiável e sem a ocorrência de mudanças. Além disso, assegura que a informação não seja modificada, gravada ou excluída sem autorização ou acidentalmente;

III – Confidencialidade: garante que a informação seja acessível apenas às pessoas físicas, ao sistema e às entidades autorizadas;

IV – Autenticidade: garante a identificação de pessoa física, sistema e entidade que produziu, expediu, modificou ou excluiu a informação;

V – Proteção: assegura o direito individual e coletivo das pessoas à inviolabilidade da sua intimidade e ao sigilo da informação, nos termos previstos na Constituição Federal.

VI – capacitação das equipes envolvidas em tecnologias sensíveis;

VII – criação, desenvolvimento e manutenção de cultura relacionada à segurança da informação, alinhadas às diretrizes nacionais de segurança da informação.

Art. 8º As ações de Segurança da Informação, no âmbito do CRCSC, são norteadas pelos seguintes princípios:

I – Criticidade: define a importância da informação para a continuidade da execução das finalidades institucionais;

II – Celeridade: garante respostas rápidas a incidentes e falhas de segurança;

III – Clareza: define que as regras e a documentação sobre segurança da informação devam ser elaboradas de forma clara, precisa, concisa e de fácil entendimento;

IV – Ética: preserva o direito do empregado, colaborador, terceirizado, conselheiro, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação;

V – Legalidade: devem ser levadas em consideração as leis, as normas e as políticas organizacionais, administrativas, técnicas e operacionais vigentes;

VI – Responsabilidade: define que os usuários são responsáveis pelo cumprimento desta PSI e devem respeitar a legislação e normas pertinentes à Segurança da Informação vigentes.

VII – Privacidade: estabelece que o direito do cidadão de não ter registros pessoais e da vida privada divulgados sem sua prévia autorização devem ser assegurados; e

VIII – Publicidade: determina que a divulgação das informações deve observar os critérios legais aplicáveis.

Art. 9º São observados, ainda, sem prejuízo dos demais, os princípios constitucionais e demais normativos que regem a matéria.

Seção IV
DA ABRANGÊNCIA

Art. 10. O disposto neste instrumento aplicar-se-á a todos os empregados,

estagiários, prestadores de serviços, conselheiros e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCSC e que tenham acesso a qualquer informação ou comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

§ 1º Os contratos, convênios e instrumentos congêneres conterão cláusulas específicas que imponham aos contratados e convenentes a obrigação de observarem o disposto nesta PSI, para o exercício de suas atividades no âmbito do CRCSC.

§ 2º Os termos aditivos dos contratos, convênios e instrumentos congêneres celebrados após a aprovação desta PSI deverão incluir cláusulas específicas que imponham aos contratados/convenentes a obrigação de observarem o disposto nesta Política, para o exercício de suas atividades no âmbito do CRCSC.

CAPÍTULO II
DOS CONCEITOS E CLASSIFICAÇÃO DAS INFORMAÇÕES

Seção I
DOS CONCEITOS E DAS DEFINIÇÕES

Art. 11. Para os efeitos desta Política de Segurança, entende-se por:

I – Ameaça: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, integridade, autenticidade e disponibilidade da informação;

II – Assinatura digital: conjunto de dados criptografados, associados a determinado documento ou arquivo que foi assinado, destinado a garantir a autenticidade e a integridade das informações constantes do documento, sua autoria e eventuais modificações;

III – Acessibilidade: facilidade no acesso ao conteúdo e ao significado de um objeto digital;

IV – Ativo de informação: patrimônio composto de dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho;

V – Metadados: dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

VI – Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por um determinado indivíduo, entidade ou processo;

VII – Banco de Dados (ou Base de Dados): um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

VIII – Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

IX – Cópia de Segurança (backup): guarda de dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade.

X – Fidedignidade: credibilidade de um documento arquivístico como uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;

XI – Comitê de Tecnologia e Segurança da Informação (CTSI): grupo de pessoas designado com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do CRCSC ;

XII – Computação em nuvem: modelo computacional que permite acesso, por

demanda e independente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

XIII – Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XIV – Custódia: responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade.

XV – Custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, ou seja, recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

XVI – Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduo, entidades ou processos;

XVII – Dispositivos móveis: equipamentos portáteis, dotados de capacidade computacional e dispositivos removíveis de memória para armazenamento, entre eles, *notebooks, netbooks, smartphones, tablets, pen drives, USB drives*, HD externos e cartões de memória;

XVIII – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ou Comitê de Gestão de Riscos: grupo de pessoas designado com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança;

XIX – Evento: Acontecimento que acarrete a mudança do estado atual de um processo;

XX – Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas finalidades institucionais, caso essas ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes envolvidas, a reputação e a marca da organização, assim como seus processos e seu valor agregado. É o resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas, *softwares, hardwares*, infraestrutura, etc.) por ele utilizados;

XXI – Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação;

XXII – Gestão de Riscos em Segurança da Informação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXIII – Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do CRCSC ;

XXIV – Incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

XXV – Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independetemente do meio em que resida ou da forma pela qual seja veiculado;

XXVI – Integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

XXVII – Documento arquivístico: documento produzido ou recebido no curso de

uma atividade prática como instrumento ou resultado dessa atividade, retido para ação ou referência;

XXVIII – Inventário e Mapeamento de Ativos de Informação: processo interativo e evolutivo, composto de três etapas:

a) identificação e classificação de ativos de informação;
b) identificação de potenciais ameaças e vulnerabilidades; e
c) avaliação de riscos.

XXIX – *Malwares*: o nome *malware* vem do inglês *malicous software* (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao seu dispositivo;

XXX – Preservação digital: conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário;

XXXI – Repositório digital: complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos;

XXXII – Repositório arquivístico digital: repositório digital que armazena e gerencia documentos arquivísticos, seja nas idades corrente e intermediária, seja na idade permanente;

XXXIII – Plano de Continuidade de Serviços Essenciais: documentação dos procedimentos e informações necessários para manter os ativos de informação críticos e a continuidade de suas atividades em local alternativo previamente definido, em casos de incidentes;

XXXIV – Plano de Recuperação de Serviços Essenciais: documentação dos procedimentos e informações necessários para que se operacionalize o retorno das atividades críticas à normalidade;

XXXV – Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

XXXVI – Público-Alvo: conjunto de usuários internos e externos atendidos pela Equipe de Tratamento e Resposta a Incidentes;

XXXVII – Recurso Criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXXVIII – Risco: possibilidade potencial de uma ameça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

XXXIX – Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XL – Serviços Essenciais: são aqueles que são imprescindíveis à atividade finalística deste Conselho;

XLI – Spam: termo usado para referir-se a *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.

XLII – Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XLIII – Termo de Confidencialidade: documento formal assinado por prestadores de serviço do CRCSC, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes;

XLIV – Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XLV – Trilhas de Auditoria: são rotinas específicas programadas nos sistemas

para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (*logs*) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

XLVI – Unidade Gestora de Segurança da Informação: é a unidade responsável pela gestão de segurança da informação no CRCSC;

XLVII – Unidades Organizacionais: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz;

XLVIII – Usuários: pessoa física ou jurídica que opera algum sistema informatizado do Conselho Regional de Contabilidade de Santa Catarina (CRCSC);

XLIX – Vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças;

L – Phishing: também conhecido como roubo de identidade. É uma fraude eletrônica, na qual o criminoso cibernético tenta obter informações confidenciais de forma fraudulenta. Normalmente, é realizado por falsificação de e-mail ou mensagem instantânea, e, muitas vezes, direciona usuários a inserir informações pessoais em um site falso, que corresponde à aparência do site legítimo. Esse método é muito usado para roubar senhas e números de cartões de crédito, entre outros dados confidenciais.

Seção II
DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 12. A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrange informações provenientes dos serviços essenciais de Tecnologia da Informação do CRCSC.

Parágrafo único. As informações devem ser classificadas de forma a permitir tratamento diferenciado de acordo com o seu grau de importância, criticidade, sensibilidade e em conformidade com requisitos legais.

Art. 13. As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

I – Pública: são informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete a execução das finalidades institucionais e que, por isso, não necessitam de proteção efetiva ou tratamento específico, em especial, editais de licitação, agendas e rotinas;

II – Interna: são informações disponíveis aos colaboradores do CRCSC para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo, em especial, memorandos, procedimentos internos, avisos e campanhas internas;

III – Confidencial: são informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros, em especial, processos judiciais e dados cadastrais de

colaboradores;

IV – Confidencial/Restrita: são informações de acesso restrito a um colaborador ou grupo de colaboradores que, obrigatoriamente, são delas destinatários. Em geral, informações associadas ao interesse estratégico do CRCSC e estão restritas ao presidente, ao(à) diretor(a), aos coordenadores, aos gerentes e aos colaboradores, cujas funções requeiram conhecê-las, em especial, resultado da avaliação de desempenho-

CAPÍTULO III
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
DAS COMPETÊNCIAS

Art. 14. Ao Comitê de Tecnologia e Segurança da Informação (CTSI) compete:

I – propor melhorias e atualizar a Política de Segurança da Informação (PSI);

II – propor, analisar e revisar normas complementares relativas à segurança da informação, em conformidade com as legislações vigentes e submeter a aprovação ao Conselho Diretor do CRCSC;

III – tratar dos assuntos de Segurança da Informação e assessorar diretamente as decisões do Conselho Diretor do CRCSC;

IV – propor investimentos relacionados à segurança da informação com o intuito de fortalecer o ambiente tecnológico e não digital e minimizar os riscos causados em virtude de possíveis vulnerabilidades;

V – classificar e reclassificar o nível de acesso às informações sempre que necessário;

VI – acompanhar o gerenciamento do ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;

VII – coordenar as atividades de tratamento e resposta a incidentes de segurança;

VIII – promover a recuperação de sistemas;

IX – agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de Segurança da Informação e avaliando condições de segurança de rede por meio de verificações de conformidade;

X – realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

XI – receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores e em suportes físicos do CRCSC;

XII – executar as ações necessárias para tratar quebras de segurança;

XIII – obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes.

XIV - planejar e coordenar a execução das ações de Segurança da Informação;

XV - definir estratégias para a implementação desta Política de Segurança da Informação (PSI) e suas normas complementares;

XVI - supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de Segurança da Informação;

XVII - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas;

XVIII - encaminhar os fatos apurados, decorrentes de quebras de segurança, para a aplicação das penalidades previstas;

XIX - gerenciar a análise de risco;

XX - verificar se os procedimentos de Segurança da Informação estão sendo aplicados de forma a atender à conformidade com legislações vigentes; e

XXI - providenciar a divulgação interna e permanente desta PSI e de suas normas complementares.

Art. 15. À Coordenadoria do Departamento de TI compete:

I – planejar, coordenar, supervisionar, executar e controlar as atividades de TI em conformidade com as diretrizes desta PSI;

II – elaborar, implementar e atualizar normas internas específicas em conformidade com esta PSI e demais diretrizes do Conselho;

III – propor as metodologias e processos referentes à segurança da informação, como classificação de acessos à informação, avaliação de risco, análise de vulnerabilidade, entre outros;

IV – gerenciar o ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;

V – manter registros e procedimentos como trilhas de auditoria e outros que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso a todos os sistemas corporativos e das redes computacionais do CRCSC;

VI – manter equipe, interna ou terceirizada, de Segurança da Informação com a responsabilidade de apoiar o Comitê de Tecnologia e Segurança da Informação (CTSI) no cumprimento de suas atribuições.

VII – definir as regras para instalação de software e hardware no CRCSC;

VIII – avaliar a possibilidade de utilização de equipamentos pessoais (*smartphones* e *notebooks*) para uso na rede do CRCSC, condicionado ao cumprimento dos requisitos de segurança que garantam a integridade das informações;

IX – supervisionar os acessos às informações e aos ativos de tecnologia (sistemas, banco de dados, recursos de rede), tendo como referência a PSI e as normas de segurança da informação;

X – efetuar as alterações, exclusões, inclusões e manter registro e controles atualizados de todos os acessos sempre que demandado formamelmente pelas Unidades Organizacionais acerca de admissão, demissão e movimentação de pessoal e/ou entrada/saída de novos processos;

XI – promover, com o envolvimento do Comitê de Gestão de Pessoas, palestras de conscientização dos colaboradores em relação à importância da segurança da informação;

XII – manter comunicação efetiva com o Comitê de Tecnologia e Segurança da Informação (CTSI) sobre possíveis ameaças e ações que deverão ser adotadas para mitigação dos riscos;

XIII – buscar alinhamento com as diretrizes da organização, em especial com o planejamento estratégico, Plano Diretor de Tecnologia da Informação (PDTI), e Plano de Integridade.

Art. 16. Ao Departamento Contábil-financeiro (área de Pessoal) compete:

I – comunicar ao Departamento de Tecnologia da Informação o ingresso, a alteração de lotação ou localização, bem como o desligamento de pessoal, inclusive postos terceirizados, no âmbito do CRCSC.

Seção II

DAS RESPONSABILIDADES

Subseção I
DOS USUÁRIOS

Art. 17. Para o Conselho Regional de Contabilidade de Santa Catarina, são considerados usuários todos os conselheiros, integrantes de grupos de trabalhos, empregados, estagiários, prestadores de serviços e terceiros que tenham acesso ao ambiente de tecnologia da informação e têm as seguintes responsabilidades:

I – ter pleno conhecimento e cumprir fielmente a PSI, as normas e os procedimentos de segurança da informação do CRCSC;

II – solicitar esclarecimentos ao Comitê de Tecnologia e Segurança de Informação (CTSI) em caso de dúvidas relacionadas à PSI;

III – gerenciar os ativos sob sua responsabilidade e garantir que os documentos e arquivos impressos ou digitais, equipamentos e recursos tecnológicos à sua disposição sejam utlizados, exclusivamente, para uso a serviço do CRCSC;

IV – acessar a rede de dados do CRCSC somente após tomar ciência das normas de Segurança da Informação e assinar o Termo de Responsabilidade;

V – tratar a informação arquivística digital e impressa como patrimônio do CRCSC e como recurso que deva ter seu sigilo preservado;

VI – utilizar as informações arquivísticas digitais e impressas disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do CRCSC exclusivamente para o interesse do serviço;

VII – preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

VIII – não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança ou cujo teor não tenha autorização ou necessidade de conhecer;

IX – não se fazer passar por outro usuário usando a identificação com login e senha de acesso;

X – no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;

XI – não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional do CRCSC por terceiros;

XII – responder perante o CRCSC pelo uso indevido das suas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil;

XIII – não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

XIV – não transferir qualquer tipo de arquivo que pertença ao CRCSC para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

XV – estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço não são permitidos na rede computacional do CRCSC;

XVI – estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional e nos arquivos setoriais, intermediários e permanentes impressos ou digitais do CRCSC pode ser auditada;

XVII – estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional do CRCSC deve obedecer a esse preceito;

XVIII – assinar o Termo de Responsabilidade – Anexo I e declarar, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PSI;

XIX – utilizar as credenciais de acesso, login e senha, e os recursos computacionais,

em conformidade com a PSI do CRCSC e procedimentos estabelecidos em normas específicas do Conselho;

XX – comunicar, tempestivamente, ao gestor imediato ou ao Comitê de Segurança da Informação qualquer violação a esta política, suas normas e procebimentos;

XXI – fazer uso da política de mesa limpa e tela protegida para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho.

XXII - devolução das informações ou documentos sigilosos que estejam em seu poder

XXIII - eliminação completa de dados digitais que porventura foram armazenados em seus equipamentos eletrônicos e *softwares* de uso particular e e-mails pessoais.

Subseção II
DO CUSTODIANTE

Art. 18. Ao Custodiante da Informação cabem as seguintes responsabilidades:

I – cumprir e zelar pela observância integral das diretrizes desta PSI e demais normas e procedimentos decorrentes;

II – zelar pela disponibilidade, integridade e confidencialidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta PSI e demais normas e procedimentos decorrentes, mediante assinatura do Termo de Responsabilidade;

III – participar de capacitação e treinamento em segurança da informação, quando convocado;

IV – utilizar os recursos sob sua responsabilidade, exclusivamente, para o fim a que se destinam;

V – proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

VI – preservar a classificação do grau de sigilo de documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções; e

VII – comunicar prontamente ao seu gestor imediato e ao Comitê de Segurança da Informação qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, a integridade e a confidencialidade das informações.

Subseção III
DOS GESTORES DAS UNIDADES ORGNACIONAIS

Art. 19. Os gestores das unidades organizacionais do CRCSC são responsáveis por:

I – ter postura exemplar em relação à segurança da informação para servir como modelo de conduta para os colaboradores sob sua gestão;

II – cumprir e fazer cumprir esta PSI;

III – exigir das entidades relacionadas, prestadores de serviços ou outras entidades externas, a assinatura do Termo de Confidencialidade referente às informações as quais terão acesso;

IV – informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

V – adotar os procedimentos necessários sempre que identificar descumprimentos da PSI.

CAPÍTULO IV

DAS DIRETRIZES E PROCEDIMENTOS

Seção I
DAS DIRETRIZES

Art. 20. Esta PSI tem como principal diretriz a preservação da disponibilidade, integridade e confiabilidade dos dados, informações e conhecimentos que compõem o ativo da informação do CRCSC.

Art. 21. Os usuários deverão ser treinados e conscientizados nos procedimentos de segurança da informação.

Art. 22. Quando do afastamento, da mudança de responsabilidade, de lotação ou de atribuições do usuário dentro da organização, far-se-á necessária a revisão imediata dos direitos de acesso e uso dos ativos.

§ 1º Os direitos de acesso e o uso dos ativos atribuídos ao usuário deverão ser extintos quando da efetivação de seu desligamento.

§ 2º Todo ativo produzido pelo usuário desligado será de propriedade do CRCSC, observadas as disposições da legislação aplicável.

Subseção I
DOS PRESSUPOSTOS BÁSICOS

Art. 23 Esta Política de Segurança da Informação é constituída dos seguintes pressupostos básicos:

I – o sucesso das ações nos assuntos de segurança da informação está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas;

II – a informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado;

III – a Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, de disponibilidade e de confidencialidade;

IV – todos os empregados, estagiários, conselheiros e prestadores de serviços, membro de grupos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do CRCSC e sejam usuários dos ativos sigilosos devem assinar o Termo de Responsabilidade quanto ao sigilo dos dados, informações e conhecimentos da administração do CRCSC.

Seção II
DAS PROVIDÊNCIAS

Subseção I
DO TRATAMENTO DA INFORMAÇÃO

Art. 24. Esta Política de Segurança da Informação considera os seguintes requisitos para o Tratamento da Informação:

I – toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade do CRCSC e deve ser protegida segundo as diretrizes descritas nesta PSI e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços institucionais e preservar sua imagem;

II – é expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo CRCSC;

III – os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos das finalidades institucionais do CRCSC;

IV – as informações criadas, armazenadas, manuseadas, transportadas ou descartadas devem ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas internas e legislação específica em vigor;

V – todo usuário deve respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas;

VI – as informações produzidas ou custodiadas pelo CRCSC somente devem ser descartadas ou destruidas conforme o seu nível de classificação e atendendo às exigências legais;

VII – deve ser disponibilizada uma solução de Gestão Eletrônica de Documentos com mecanismos de assinatura digital aderente à legislação em vigor, com a finalidade de mitigar riscos associados à informação impressa;

VIII – a manipulação de informações classificadas em qualquer grau de sigilo deve seguir as normas internas e a legislação em vigor;

§ 1º Qualquer outra forma de uso das informações que extrapole as atribuições necessárias ao desempenho das atividades dos usuários, internos ou colaboradores, necessitará de prévia autorização formal.

§ 2º O acesso, quando autorizado, dos usuários internos ou externos às informações produzidas ou custodiadas pelo CRCSC, que não sejam de domínio público, será condicionado a um termo de sigilo e responsabilidade, formal ou virtual.

Parágrafo único. As informações deverão ser classificadas de forma a permitir tratamento diferenciado de acordo com seu grau de importância, criticidade, sensibilidade, e em conformidade com requisitos legais.

Subseção II
DA UTILIZAÇÃO DA REDE

Art. 25. O ingresso à rede interna deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minizados, devendo os procedimentos serem definidos em normas específicas, em especial, a Política de Controle de Acesso Lógico do CRCSC.

Subseção III
DO TRATAMENTO DE INCIDENTES DE REDE

Art. 26. Tratamento de Incidentes de Rede:

I – a gestão de incidentes de segurança da informação deverá ser realizada por meio de processo formalizado, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança;

II – o Departamento de Tecnologia da Informação (DTI) manterá Equipe de

Tratamento e Resposta a Incidentes em Redes Computacionais, com a responsabilidade de receber, analisar e responder a notificações e a atividades relacionadas a incidentes de segurança em rede de computadores;

III – sua criação, sua estrutura e seu modelo de implementação serão definidas em Portaria que deverá estar em conformidade com as diretrizes desta PSI.

Subseção IV
DA GESTÃO DE RISCOS

Art. 27 Gestão de Riscos:

I – a gestão de riscos é realizada por meio de processo formalizado, contendo as fases de análise, avaliação e tratamento dos riscos;

II – os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica sobre gestão de riscos em segurança da informação;

III – os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito do CRCSC;

IV – o processo de inventário e mapeamento de ativos de informação deve ser aplicado tanto na gestão de riscos quanto na gestão de continuidade, conforme procedimentos definidos em norma específica sobre o tema.

Subseção V
DA GESTÃO DE CONTINUIDADE

Art. 28. Gestão de Continuidade:

I – o CRCSC deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

II – as informações de propriedade ou custodiadas pelo CRCSC, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança atualizada e guardada em local remoto, de forma a garantir a continuidade das atividades do órgão.

III – as informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

IV – as diretrizes para a Gestão de Continuidade de de TI em Segurança da Informação, conforme procedimentos definidos em norma específica, deve minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades críticas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

Subseção VI
DA AUDITORIA E CONFORMIDADE

Art. 29. Auditoria e Conformidade:

I – a Auditoria em Segurança da Informação é uma atividade devidamente estruturada para examinar criteriosamente a situação dos controles que se aplicam à segurança da informação, especialmente por meio da análise de objetos e respectivos pontos de controle. Para tanto, é preciso verificar que os controles estejam de acordo com as normas e políticas de segurança estabelecidas para esses ativos, bem como se o que está em operação alcança os objetivos de segurança;

II – o CRCSC deve criar e manter registros e procedimentos, como trilhas de

auditoria, que possibilitem o rastreamento, o acompanhamento, o controle e a verificação de acessos aos sistemas corporativos e rede interna da entidade;

III – deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de Segurança da Informação aplicadas no CRCSC com esta PSI, bem como com a legislação específica em vigor;

IV – a verificação de conformidade deve ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o CRCSC;

V – a verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros e logs, análise de código-fonte, entrevistas e testes de invasão;

VI – os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade;

VII – os procedimentos e as metodologias utilizados na auditoria e conformidade no âmbito do CRCSC serão definidos em norma específica, em conformidade com as diretrizes desta PSI e demais legislações em vigor;

VIII – as medidas de proteção para que administradores de sistemas não tenham permissão de exclusão ou desativação de registros de log de suas próprias atividades deverão ser tomadas;

IX – os recursos e informações de registro de log deverão ser protegidos contra falsificação e acesso não autorizado;

X – compete ao Sistema de Gestão da Qualidade do CRCSC o acompanhamento da Auditoria de Segurança da Informação.

Subseção VII
DO CONTROLE DE ACESSO

Art. 30. Controle de Acesso:

I – o controle de acesso aos sistemas internos e externos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico e serão definidos em norma específica, em conformidade com as diretrizes desta PSI;

II – as medidas de proteção serão adotadas para evitar que usuários dos ativos de Tecnologia da Informação não tenham permissão para instalar, remover, modificar, criar ou desenvolver softwares sem a devida autorização.

Subseção VIII
DA POLÍTICA DE SENHAS

Art. 31. A política de senhas de acessos aos sistemas e informações do CRCSC deve ser definida em norma específica, Política de Controle de Acesso Lógico do CRCSC – Aprovada Resolução N.º 444/2021, em conformidade com as diretrizes desta PSI.

Subseção IX
DO USO DE E-MAIL

Art. 32. O uso de *e-mail* no âmbito do CRCSC deve ser definido em norma específica, em conformidade com as diretrizes desta PSI, e deve tratar, entre outras coisas, do

controle de acesso.

Subseção X
DO ACESSO À INTERNET

Art. 33. O acesso à rede mundial de computadores, no âmbito do CRCSC, deve ser definido em norma específica, em conformidade com as diretrizes desta PSI, orientações governamentais e legislações específicas em vigor.

Subseção XI
DO INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 34. Inventário e Mapeamento de Ativos de Informação:

I – nos aspectos relacionados à Segurança da Informação, o processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios para a Gestão de Segurança da Informação, Gestão de Riscos de Segurança da Informação, Gestão de Continuidade de TI, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas, de auditoria e, principalmente, de estruturação e de geração da base de dados sobre os ativos de informação;

II – o processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação;

III – o inventário deve documentar e classificar a importância do ativo para as finalidades institucionais, o impacto para atividades finalísticas em caso de comprometimento e a estratégia que permita a recuperação do ativo em caso de desastre;

IV – todos os ativos críticos devem ter um proprietário formalmente designado.

V– o proprietário dos ativos de informação é a parte interessada do CRCSC, ou indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

VI – o proprietário é responsável por:

a) assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificados;

b) definir e periodicamente analisar criticamente as classificações e as exigências de segurança da informação para os ativos de informação;

c) identificar os riscos e comunicar as exigências de segurança da informação para os ativos sob sua responsabilidade aos custodiantes e usuários;

d) implementar controles internos a fim de verificar se as exigências estão sendo cumpridas.

VII – o proprietário do ativo pode delegar formalmente as tarefas de rotina a um custodiante que cuida do ativo no dia a dia, porém a responsabilidade permanece do proprietário;

VIII – o custodiante dos ativos de informação é qualquer indivíduo ou estrutura que tenha a responsabilidade formal de proteger um ou mais ativos de informação. É responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação informadas pelo proprietário dos ativos de informação;

IX – as regras para uso dos ativos associados com a informação e dos recursos de processamento da informação devem ser identificadas, documentadas e implementadas;

X – os usuários que têm acesso aos ativos do CRCSC devem estar conscientes dos requisitos de segurança da informação;

XI – a informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada;

XII – o proprietário do ativo de informação deve ser responsável por sua classificação.

Subseção XII
DOS DISPOSITIVOS MÓVEIS

Art. 35. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito do CRCSC deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário e ser definido em norma específica em conformidade com as diretrizes desta PSI.

Subseção XIII
DA COMPUTAÇÃO EM NUVEM

Art. 36. A implementação ou contratação de computação em nuvem no âmbito do CRCSC deve ser definida em norma específica, em conformidade com as diretrizes desta PSI e com as demais legislações vigentes sobre o tema.

Subseção XIV
DO *BACKUP*

Art. 37. Todo sistema ou informação relevante para a operação das finalidades institucionais do CRCSC deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição, devendo a implementação dos procedimentos de *backups* ser definida em norma específica.

Subseção XV
DA CRIPTOGRAFIA

Art. 38. Criptografia:

I – a cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico, conforme procedimentos definidos em norma e legislações específicas em vigor;

II – qualquer sistema próprio do CRCSC que contenha tabelas com senhas devem ter essas tabelas armazenadas de forma criptografada.

Subseção XVI
DAS REDES SOCIAIS

Art. 39. O uso institucional das redes sociais deve ser norteado por diretrizes, critérios, limitações e responsabilidades, definidas em norma complementar, em conformidade com as diretrizes desta PSI.

Subseção XVII
DA CONTRATAÇÃO DE SERVIÇOS

Art. 40. Contratação de Serviços:

I – nos editais de licitação e nos contratos de empresas prestadoras de serviços com o CRCSC, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta PSI, bem como ser exigida da empresa contratada e do prestador de serviços a assinatura do Termo de Responsabilidade e do Termo de Confidencialidade;

II – a empresa contratada também deverá demonstrar que possui mecanismos que

assegurem a segurança das informações do CRCSC por ela acessadas, direta ou indiretamente, acesso aos ativos que contêm informações, e cumprir o disposto nesta PSI quando aplicável;

III – não poderá ser objeto de contratação a Gestão de Processos de Tecnologia da Informação ou a Gestão de Segurança da Informação;

IV – o apoio técnico aos processos de planejamento e a avaliação da qualidade das soluções de tecnologia da informação poderão ser objetos de contratação, desde que sob supervisão exclusiva de empregados do CRCSC;

V – os termos e procedimentos para contratação de serviços terceirizados serão detalhados em norma complementar específica.

CAPÍTULO V
DA DIVULGAÇÃO E ATUALIZAÇÃO

Art. 41. Esta PSI e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários e disponibilizadas no portal do CRCSC, sendo consideradas um documento de relevante interesse público.

Art. 42. Esta Política de Segurança da Informação deverá ser revisada a cada 2 (dois) anos ou sempre que se fizer necessário, não excedendo ao período máximo de 3 (três) anos, a contar da data de sua publicação.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 43. A inobservância dos dispositivos constantes desta Política de Segurança da Informação pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 44. Os casos omissos desta PSI serão resolvidos pelo Comitê de Tecnologia e Segurança da Informação do CRCSC.

Art. 45. O Conselho Regional de Contabilidade tem o prazo de 24 (vinte e quatro) meses para implementação de todas as ações propostas por esta Política de Segurança da Informação.

ANEXO I

Termo de Responsabilidade

Pelo presente termo, eu, _____, declaro ter conhecimento da Política de Segurança da Informação do Conselho Regional de Contabilidade de SC (CRCSC), disponível para consulta na intranet (*link*....).

Declaro que estou recebendo uma conta com privilégios adequados ao exercício das atividades que executo, a qual será utilizada somente para tal fim.

Declaro estar ciente de que minhas ações serão monitoradas nos termos da Política de Segurança da Informação do CRCSC e de que qualquer alteração será de minha responsabilidade, feita a partir de minha identificação, autenticação e autorização.

Estou ciente, ainda, que serei responsável pelo dano que possa causar em caso de descumprimento da Política de Segurança da Informação do CRCSC, ao realizar uma ação de iniciativa própria de tentativa quanto à modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Florianópolis (SC), ____ de _____ de 20XX.

Nome:
Matrícula:
Unidade Organizacional:

Nome:
Unidade Organizacional:
(titular da unidade organizacional ou gestor do contrato, para o caso dos terceirizados)

Este documento foi assinado eletronicamente com fundamento no art. 4º,do Decreto nº 10.543, de 13 de novembro de 2020.

Signatários e datas conforme horário oficial de Brasília:

✓ MARISA LUCIANA SCHVABE DE MORAIS (CPF XXX.133.239-XX) em 08/03/2022 15:16:44