RESOLUÇÃO CRCSC N.º 485, DE 19 DE JUNHO DE 2024.

Aprova o Plano Diretor de Tecnologia da Informação (PDTI) do Conselho Regional de Contabilidade de Santa Catarina, biênio 2024 - 2025.

O CONSELHO REGIONAL DE CONTABILIDADE DE SANTA CATARINA, no exercício de suas atribuições legais e regimentais, resolve:

Art. 1º Aprovar o Plano Diretor de Tecnologia da Informação (PDTI) do Conselho Regional de Contabilidade de Santa Catarina, referente ao biênio 2024 - 2025, em atendimento ao disposto na portaria n.º 778, de 4 de abril de 2019, alterada pela portaria n.º 18.152 ,de 4 agosto de 2020, ambas da Secretaria de Governo Digital que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração do os Recursos de Tecnologia da Informação do Poder Executivo Federal (Sisp).

Art. 2º Plano Diretor de Tecnologia da Informação (PDTI) do Conselho Regional de Contabilidade de Santa Catarina está disponível no sítio www.crcsc.org.br.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

CONTADORA MARISA LUCIANA SCHVABE DE MORAIS
Presidente

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 21/06/2024 12:22:45

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO – PDTI

Departamento de Tecnologia da Informação

Maio de 2024 | Versão 1.4

Histórico de Versões

Data	Versão	Descrição	Autor
30/11/2023	1.0	Esboço	Fernando Proenço Zucatto
11/12/2023	1.1	Primeira Entrega	Fernando Proenço Zucatto
26/02/2024	1.2	Término da Metodologia e Início da Revisão Inventário Equipamentos em uso	Fernando Proenço Zucatto Fernando Vill (Inventário Equipamentos)
22/05/2024	1.3	Finalização do Cronograma Divisão de Tarefas Matriz de Conhecimento Finalização da Revisão Inventário Equipamentos em uso em dezembro/2024	Fernando Proenço Zucatto Fernando Vill (Inventário Equipamentos)
29/05/2024	1.4	Inclusão de estudos para utilização de Inteligência Artificial. Inclusão de estudos para capacitações necessárias no biênio.	Fernando Proenço Zucatto

Índice

1 INTRODUÇÃO

A governança em Tecnologia da Informação (TI) é um componente crítico para garantir que as estratégias e objetivos de uma organização estejam alinhados com o uso eficaz da tecnologia.

Um Plano Diretor de Tecnologia da Informação (PDTI) é um documento estratégico que estabelece as diretrizes, metas e ações relacionadas à gestão da tecnologia da informação em uma organização.

O Plano Diretor de Tecnologia de Informação Biênio 2024-2025, 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).

Em um mundo cada vez mais digitalizado, a governança em Tecnologia da Informação (TI) tornou-se um pilar fundamental para o sucesso das organizações. A governança em TI é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. Ela envolve liderança, estruturas organizacionais e processos que garantem que a TI da organização sustente e estenda as estratégias e objetivos da empresa.

Alinhamento Estratégico: A governança em TI assegura que os investimentos em tecnologia estejam alinhados com as metas e objetivos estratégicos do CRCSC. Isso é feito através de um planejamento cuidadoso e análise de retorno sobre investimento para projetos de TI.

Gerenciamento de Riscos: Com a governança, os riscos associados à TI, como segurança cibernética, falhas de sistema e conformidade com regulamentações, são identificados e gerenciados de forma proativa. Isso minimiza as vulnerabilidades e protege os ativos da organização.

Eficiência Operacional: A governança em TI promove a eficiência operacional ao padronizar os procedimentos e garantir que os recursos de TI sejam utilizados de maneira ótima. Isso inclui a gestão de infraestrutura, aplicações e serviços de TI.

Responsabilidade: Estabelece clareza de responsabilidades entre a TI e os outros departamentos, garantindo que todos os envolvidos compreendam seus papéis na gestão e utilização dos recursos de TI.

Inovação: Ao fornecer um framework para a tomada de decisão em TI, a governança cria um ambiente que fomenta a inovação. Isso permite que a organização se adapte rapidamente às mudanças do mercado e às novas oportunidades tecnológicas.

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 CRCSC. Tem como abrangência os anos de 2024 e 2025, sendo que deverá ser revisto sempre que a gestão julgar necessário, para acompanhamento do cronograma e correções devidas conforme demanda institucional. São pontos importantes para termos o objetivo atingido:

Alinhar a TI com os Objetivos Estratégicos: O principal objetivo do PDTI é garantir que os investimentos em TI estejam alinhados com os objetivos estratégicos do CRCSC. Ele define as prioridades e as ações necessárias para atender às necessidades de negócios por meio da tecnologia.

Planejar o Uso Eficiente dos Recursos: O PDTI estabelece um roteiro para o uso eficiente dos recursos de TI, incluindo infraestrutura, sistemas, pessoal e orçamento. Ele ajuda a evitar

desperdícios e a otimizar os investimentos.

Promover a Inovação e a Transformação Digital: O PDTI deve incentivar a inovação, identificando oportunidades para o uso estratégico da tecnologia. Ele também apoia a transformação digital da organização, permitindo a adoção de novas soluções e práticas.

Definir Responsabilidades e Processos: O PDTI atribui responsabilidades claras para a gestão da TI, incluindo papéis e processos. Isso melhora a governança e a prestação de contas.

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.

São pontos importantes que também justificam a criação deste PDTI:

Complexidade Tecnológica: A rápida evolução tecnológica exige um planejamento estruturado para lidar com a complexidade dos sistemas, aplicativos e infraestrutura de TI.

Riscos e Segurança: A falta de um plano diretor pode resultar em riscos de segurança, como vulnerabilidades cibernéticas e falhas de conformidade.

Maximização do Retorno sobre Investimento (ROI): O PDTI ajuda a priorizar projetos e investimentos que proporcionam maior retorno para a organização.

Sustentabilidade: Um PDTI bem elaborado contribui para a sustentabilidade da TI, garantindo que ela continue a atender às necessidades do CRCSC ao longo do tempo.

Em resumo, o PDTI é uma ferramenta essencial para a gestão estratégica da TI, promovendo o alinhamento, a eficiência e a inovação no uso da tecnologia da informação.

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 nas últimas décadas, 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 assistente de suporte em informática e um estagiário, são eles:

Nome	Cargo	Divisão de Trabalho*
Fernando Proença Zucatto	Coordenador do Departamento de Tecnologia da Informação	Gestão, Novos Projetos, PDTI, DFDs, *Compliance*, Riscos e Office 365.
Fernando Proença Zucatto	Coordenador do Departamento de 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.
Josef Konrad Bruseke	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 14.133/21, 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, 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

Um dos componentes cruciais do PDTI é o inventário de hardware. Aqui temos que salientar a importância desse inventário e como ele contribui para o sucesso do negócio:

Controle de Recursos: O inventário de hardware permite um controle rigoroso dos ativos tecnológicos do CRCSC. Isso inclui computadores, servidores, dispositivos de rede e outros equipamentos. Ter um registro detalhado desses recursos facilita a organização e ações dos profissionais do Departamento de TI.

Manutenção e Suporte: Com um inventário atualizado, o suporte técnico pode identificar rapidamente os dispositivos, diagnosticar problemas e realizar manutenções preventivas. Isso aumenta a vida útil dos equipamentos e melhora a eficiência operacional.

Segurança: O inventário ajuda a identificar vulnerabilidades de segurança. Dispositivos desatualizados ou sem patches podem representar riscos. Manter um inventário preciso permite que a equipe de TI tome medidas proativas para proteger a rede e os dados.

Planejamento Estratégico: O inventário de hardware é fundamental para o planejamento de longo prazo. Ele fornece informações sobre a capacidade atual e futura da infraestrutura de TI. Com base nesses dados, o CRCSC pode tomar decisões informadas sobre investimentos em novos equipamentos e atualizações.

Em resumo, o inventário de hardware no PDTI é uma ferramenta poderosa para otimizar recursos, melhorar a segurança e garantir o alinhamento da TI com os objetivos de negócio.

A tabela abaixo detalha os equipamentos em uso até dezembro de 2023:

Hardware	Data de Aquisição	Quantidade
Access Point Unifi AC UAP LR Ubiquiti	2020	10
Camera IP HD Hikvision 2 Mega	2022	22
Desktop Montado Intel i5	2010	2
Desktop HP Compaq 8200	2011	6
Desktop HP Compaq 8200	2012	12
Desktop HP Compaq 6300	2013	6
Desktop HP Elitedesk800 G2 SFF	2017	24

HD Externo	-	21
Impressora Epson Lx300	-	4
Impressora HP M1120	2009	3
Impressora Térmica Argox	2010	1
Impressora Brother Color HL4150CDN	2014	1
Impressora HP DeskJet 3546	2014	1
Impressora HP OfficeJet Mobile 200	2019	1
Mesa Digitalizadora OneByWacom CTL472	2020	3
Monitor Samsung 17	2008	6
Monitor LG 19	2010	5
Monitor LG 18.5	2011	1
Monitor HP w1905G	2011	1
Monitor TV Samsung 21	2012	2
Monitor HP L200HX	2012/2013	1
Monitor AOC 19,5 E2050swn	2014	10
Monitor Tv LG 23.6	2016	2
Monitor HP 23 E232	2017	24
Monitor HP 23,6 V24b	2019	4
Monitor Samsung 27	2019	1
Notebook HP PAVILION DV2765	2008	1
Notebook HP PROBOOK 4310s	2009/2010	9
Notebook HP 6460B	2012	7
Notebook HP 8460P	2012	1
Notebook Lenovo ThinkPad x240	2015	1
Notebook Inspiron 15 7572	2018	1
Notebook Dell Vostro 3481	2019	1
Notebook Vaio FE14	2020	1
Notebook Lenovo ThinkPad k14	2023	1
NVR Hikvision 16CH	2022	2
PROJETOR MULTIMIDIA SONY VPL EX7	2010	2
PROJETOR MULTIMÍDIA WIRELESS EPSON X36	2016	6
PROJETOR EPSON POWERLITE W49	2023	3
Rack Servidor	2015	4

Scanner Canon 3010-C	2009/2012	3
Scanner Fujtisu FI6110	2012	2
Scanner Canon DR M140	2017	1
Scanner HP G2710	2018	1
Scanner Kodak Alaris S2070	2020	7
Scanner Canon DR M160II	2023	3
Servidor Montado c/Arquitetura Desktop	-	3
Servidor Dell (R640)	2017	2
Storage NAS	2023	1
Switch Voice Panel 50 portes Cat3	2015	3
Switch Servidores	2015	3
Switch HP 5500-24G EL JD3377A	2015	2
Switch HP 1920-24G POE	2015	2
Switch Hikvision 24ch	2022	1
Tablet (IPAD 2)	2012	2
Terminal de Auto Atendimento	2016	1
Totem Multimidia	2017	1
Workstation HP Z2 G4	2019	3

2.3.3 Software

O inventário de software também é um componente fundamental do Plano Diretor de Tecnologia da Informação (PDTI). Aqui temos que salientar a importância desse inventário e como ele contribui para o sucesso do negócio:

Antecipação de Problemas: O inventário de software permite antecipar problemas técnicos. Com informações atualizadas, é possível prever questões que podem surgir, como softwares desatualizados ou vulnerabilidades.

Detecção de Softwares Maliciosos: Ao manter um inventário atualizado, o gestor de TI pode identificar softwares instalados inadvertidamente. Isso ajuda a evitar a propagação de software malicioso na rede.

Controle do Suporte e da Garantia: O inventário facilita o controle dos contratos de suporte e garantia de software. Isso garante que os prazos sejam cumpridos e que os recursos estejam disponíveis quando necessário.

Controle de Uso: Com o inventário, é possível monitorar o uso de licenças de software. Isso evita gastos desnecessários e ajuda na conformidade com as políticas de licenciamento.

A tabela abaixo detalha os sistemas em uso até dezembro de 2023:

Software Licenciados	Área de Negócio	Quantidade de Licenças
Microsoft 365 Business Basic	Informática	08 (oito)
Microsoft 365 Business Standard	Informática	66 (sessenta e seis)
Microsoft Power BI Pro	Informática	4 (quatro)
TeamViewer Licença Corporate	Informática	1 (uma)
Windows Server 2016	Informática	10 (dez)
Adobe Creative Cloud	Comunicação	4 (quatro)
Adobe Premiere Pro	Comunicação	1 (uma)
Corel Draw	Comunicação	6 (seis)
CP-Pro	Jurídico	8 (oito)
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)
SQL Server 2017	Informática	2 (duas)
SophiA Biblioteca nº série 8556	Desenvolvimento Profissional	1 (uma)
Adobe Acrobat X Pro	Desenvolvimento Profissional	3
Adobe Acrobat XI Pro	Fiscalização	1
WTS - Acesso remoto (Perpétua)	Informática	17
Zoom Meeting Profissional	Desenvolvimento	1
StreamYard Basic	Desenvolvimento	1
Adobe Acrobat PRO DC	Informática	20
Windows 11 Professional OEM	Informática	15

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".

Outro ponto importante relacionado a estrutura de TI veio com a unificação do contrato entre a fornecedora de software SPW e o CFC ocorrida em dezembro/2023, estão sendo promovidas diversas mudanças para adequação do sistema unificado em todos os estados, uma delas é a migração de todas as bases de dados dos estados para o ambiente em nuvem criado pelo CFC. O CRCSC está atento a tais intenções de mudanças e com estudos em andamento para os prováveis cenários, buscando assim melhor aproveitar a estrutura física já existente.

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
Willian Schmitt	Coordenador do Comitê
Itelvino Schinaider	Conselheiro do CRCSC e VP de Administração
Cleber Dias	Diretor de Administração e Infraestrutura
Carlos Vinicius Gonçalves	Coordenadora Depto. Fiscalização, Ética e Disciplina
Alexandra Somer Bernardes	Coordenadora Depto. Registro e Relacionamento
Ricardo Minatto Tonetto	Coordenador Depto. Desenvolvimento Profissional
Cláudio da Silva Petronilho	Diretor Institucional e de Relacionamento com o Profissional
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 Análise SWOT é uma ferramenta valiosa para entender o ambiente atual, identificar vantagens competitivas e tomar decisões estratégicas com base em informações sólidas, permite obter dados concretos e atualizados sobre o momento que o a organização está enfrentando. Ela abrange tanto o microambiente (forças e fraquezas internas) quanto o macroambiente (oportunidades e ameaças externas). Essa matriz pode ser alterada e atualizada conforme necessário, proporcionando flexibilidade e adaptabilidade.

Esta análise acompanha as mudanças e o crescimento da organização. Ela é versátil e possibilita a construção de um histórico, servindo como um termômetro a longo prazo para a empresa.

Ao listar os pontos fortes e fracos da empresa e identificar oportunidades e ameaças do ambiente externo, você compreende os problemas encontrados e as possibilidades de soluções a serem

implementadas. Isso ajuda na tomada de decisões mais informadas e estratégicas.

A matriz SWOT avalia cenários internos e externos, possibilitando uma visão macro do contexto atual e suas possibilidades. Ela é baseada em dados reais e tem potencial para encontrar novas oportunidades e melhorar processos ou projetos existentes.

- **FORÇAS**
  - Parque tecnológico atualizado;
  - Rápido atendimento da empresa terceirizada de consultoria em ampla variedade de suporte;
  - Grandes investimentos realizados nos últimos biênios 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, conforme regulamenta a resolução CRCSC N.º 461, de 20 de junho de 2022;
  - 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 aprimoramento da solução de Business *Intellingence*;
  - Oferta de capacitação para os empregados;
  - Avanço do projeto de Business *Intelligence*, abrangendo todos os departamentos interessados;

- **AMEAÇAS**
  - Mudança de gestão poderão acarretar alteração de prioridades;

- Novas legislações frequentes na área de segurança e proteção de dados.

6 PRINCÍPIOS E DIRETRIZES

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, para o biênio 2024-2025 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).

Ética: A atuação com integridade, celeridade, esforço, foco e responsabilidade é fundamental para o sucesso do PDTI.

Alinhamento à Estratégia de Governo Digital: O PDTI deve estar alinhado à estratégia de governo digital, garantindo que as ações de TI estejam integradas aos objetivos maiores do CRCSC.

Análise SWOT da TI: A avaliação dos pontos fortes, fracos, oportunidades e ameaças relacionados à TI é essencial para identificar fatores internos e externos que podem afetar sua capacidade de contribuir para o sucesso na aplicação das definições do PDTI.

Governança do PDTI: Estabelecer uma governança eficaz para o PDTI é crucial. Isso inclui a definição de responsabilidades, processos de tomada de decisão e acompanhamento das ações planejadas.

Priorização de Demandas: O PDTI deve priorizar demandas de sistemas, dados, segurança, privacidade e projetos estruturantes. Isso ajuda a alocar recursos de forma eficiente e a atender às necessidades mais críticas.

7 DOCUMENTOS DE REFERÊNCIA

- Modelo de Referência do Ministério da Economia - Planejamento, Desenvolvimento e Gestão;
- Plano Diretor de Tecnologia de Informação Biênio 2022-2023;
- Proposta Orçamentária e Plano de Trabalho do CRCSC de 2024;
- Portaria CRCSC nº 055/2024 Institui o Comitê de Tecnologia e Segurança da Informação (CTSI).

8 SEGURANÇA

A segurança de TI é uma prática essencial para proteger os ativos de TI de uma organização. Ela abrange uma ampla gama de medidas para evitar acesso não autorizado, violações de dados, ataques cibernéticos e outras atividades maliciosas, é fundamental para garantir a proteção dos dados confidenciais das organizações, bem como a privacidade dos clientes e a reputação da empresa.

A segurança da informação envolve um conjunto de práticas e medidas para proteger sistemas, programas, equipamentos e redes contra invasões. Ela visa evitar acessos não autorizados, roubo, perda ou danos aos dados valiosos da empresa.

No Brasil, as empresas enfrentam uma crescente quantidade de ataques cibernéticos. Em 2021, houve mais de 16 bilhões de tentativas de ataques cibernéticos às empresas brasileiras no primeiro semestre. Além disso, o país ocupa o 2º lugar no ranking mundial de ataques cibernéticos, ficando atrás apenas dos Estados Unidos, segundo constatou a pesquisa da *Netscout Threat Intelligence* em 2021.

Ataques podem afetar não apenas a operação da organização, mas também a segurança de outras pessoas envolvidas, incluindo os clientes. Exposições indevidas de dados, como o caso ocorrido durante a pandemia de COVID onde mais de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) tiveram seus dados expostos e indisponíveis para acesso em um momento de crise sanitária mundial, destacam a necessidade de proteger informações sensíveis.

Tendência e capacitação:

A cibersegurança foi apontada como uma das tendências de TI para os próximos anos. Capacitar os times para atuar nessa realidade é essencial para proteger os dados e garantir a continuidade dos negócios3.

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, estes ataques, por vezes tem altos custos para as organizações que são afetadas. Incidentes como *ransomware* e *phishing* podem exigir pagamentos caros de resgate e afetar gravemente a reputação da instituição.

A segurança de TI é crucial para proteger a confidencialidade, integridade e disponibilidade dos dados corporativos. Com a Lei Geral de Proteção de Dados (LGPD) vigorando desde agosto de 2020, as organizações precisam ficar ainda mais atentas à segurança. Afinal, elas são responsáveis 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.

Após a implantação do novo firewall, nos biênios seguintes, foi realizada segmentação da rede local em VLANs, garantindo maior segurança e acessos a servidores e demais equipamentos somente as pessoas autorizadas. 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

A Política de Segurança da Informação (PSI) é um conjunto de padrões, normas e diretrizes que estabelece princípios, compromissos, valores, requisitos e orientações com o objetivo de mitigar riscos para os dados armazenados. Essa política é especialmente importante para organizações e startups que lidam com informações confidenciais, como dados financeiros, informações de saúde ou dados de clientes.

A PSI é um documento oficial que inclui informações e regras sobre a gestão de senhas, acesso a dados, backup de dados, gerenciamento de dispositivos móveis e outras questões correlatas. Ela fornece uma camada adicional de proteção para os dados sensíveis de uma organização. Além disso, a PSI pode estabelecer diretrizes claras sobre o uso de dispositivos móveis no ambiente corporativo, incluindo o uso de criptografia e autenticação de dois fatores. Também pode incluir parâmetros sobre como lidar com eventuais incidentes, como vazamento de dados ou ameaças cibernéticas.

É importante ressaltar que a PSI não é um documento imutável. Seus padrões podem ser revisitados e atualizados de acordo com o cenário atual de cada organização. Portanto, manter a PSI atualizada e alinhada com as melhores práticas de segurança é fundamental para proteger os ativos de informação de uma organização.

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 452/2021. Tal documento encontra-se como anexo deste PDTI.

8.3. Backup e Espelhamento de Servidores

Possuir backup é fundamental para proteger os dados do CRCSC e garantir que não os percamos em caso de falhas, acidentes ou ataques cibernéticos. Pontos importantes sobre criação e armazenamento dos backups:

Prevenção de Perda de Dados: O backup regular ajuda a evitar a perda de dados valiosos. Se o seu dispositivo falhar, você ainda terá cópias dos seus arquivos.

Recuperação de Desastres: Em situações como incêndios, inundações ou roubo, o backup permite restaurar seus dados em um novo dispositivo.

Proteção contra Ransomware: Ataques de ransomware podem criptografar seus arquivos e exigir pagamento para desbloqueá-los. Com backups atualizados, podemos restaurar os dados sem pagar resgates.

Atualizações e Migrações: Ao atualizar ou trocar de dispositivo, o backup facilita a

transferência de dados.

Histórico de Versões: Alguns sistemas de backup mantêm versões anteriores dos arquivos, permitindo que você recupere versões específicas conforme necessário.

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, foi criada a política de backup das informações eletrônicas no âmbito do CRCSC, aprovada pela portaria nº 096/2022, com ela 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 dois momentos do dia, 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

Desde 2022 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 BI
2	5002	Tecnologia da Informação	437.744,00	SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO
3	5010	Modernização do Parque de Informática	165.000,00	EQUIPAMENTOS DE PROCESSAMENTO DE DADOS
4	5010	Modernização do Parque de Informática	165.000,00	LICENÇAS DE SOFTWARES

11 CRONOGRAMA DE AÇÕES 2024

#	Atividade	1º Quadrimestre	2º Quadrimestre	3º Quadrimestre	Responsável	Situação
1	Aquisição de 10 notebooks e 03 Scanners.		x		Departamento de TI	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 licenças Adobe Pro			x	Departamento de TI	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	Em Andamento
9	Renovação locação central telefônica	x			Departamento de TI	Programado
10	Renovação link telefonia sede	x			Departamento de TI	Programado
11	Renovação Link de internet Delegacias Regionais	x	x	x	Departamento de TI	Demanda
12	Dotação extra para eventuais contratações	x	x	x	Departamento de TI	Demanda
13	Renovação de sistema de suporte remoto		x		Departamento de TI	Programado

14	Revisar PDTI trimestralmente	x	x	x	Comitê PDTI	Programado
15	Capacitar equipe para módulos do SPW	x	x	x	Departamento de TI	Programado
16	Capacitação interna equipe nas tarefas operacionais como: impressoras, firewall, backup, telefonia, wifi e outras atividades rotineiras	x	x	x	Departamento de TI	Programado
17	Divulgar política de segurança da Informação e proteção de dados no CRCSC	x	x	x	Departamento de TI	Programado
18	Manutenção de hardware e sistemas	x	x	x	Departamento de TI	Demanda
19	Mapeamento processos setor de TI	x	x	x	Departamento de TI	Programado
20	Renovação consultoria *Business Intelligence(BI)*	x			Departamento de TI	Finalizado
21	Renovação Plataforma Atendimentos WhatsApp		x		Departamento de TI	Programado
22	Melhorar automação climatização Sala dos Servidores		x		Departamento de TI	Programado
23	Renovação de Licenças Corel Draw			x	Departamento de TI	Programado
24	Estudar novas tecnologias utilizando Inteligência Artificial e como aplicar ao ambiente do CRCSC		x	x	Departamento de TI	Programado
25	Estudar capacitações importantes para equipe de TI		x	x	Departamento de TI	Programado

12 PLANEJAMENTO DE AÇÕES 2025

#	Atividade	1º Quadrimestre	2º Quadrimestre	3º Quadrimestre	Responsável	Situação
1	Aquisição de 10 notebooks		x		Departamento de TI	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 licenças Adobe Pro			x	Departamento de TI	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 Link de internet Delegacias Regionais	x	x	x	Departamento de TI	Demanda
12	Dotação extra para eventuais contratações	x	x	x	Departamento de TI	Demanda
13	Renovação de sistema de suporte remoto		x		Departamento de TI	Programado
14	Revisar PDTI trimestralmente	x	x	x	Comitê PDTI	Programado
15	Capacitar equipe para módulos do SPW	x	x	x	Departamento de TI	Programado
16	Capacitação interna equipe nas tarefas operacionais como: impressoras, firewall, backup, telefonia, wifi e outras atividades rotineiras	x	x	x	Departamento de TI	Programado
17	Divulgar política de segurança da Informação e proteção de dados no CRCSC	x	x	x	Departamento de TI	Programado
18	Manutenção de hardware e sistemas	x	x	x	Departamento de TI	Demanda
19	Mapeamento processos setor de TI	x	x	x	Departamento de TI	Programado
20	Renovação consultoria *Business Intelligence(BI)*	x			Departamento de TI	Programado
21	Renovação Plataforma Atendimentos WhatsApp		x		Departamento de TI	Programado
22	Melhorar automação climatização Sala dos Servidores		x		Departamento de TI	Programado
23	Renovação de Licenças Corel Draw			x	Departamento de TI	Programado
24	Aquisição de 40 mouse/teclado sem fio	x			Departamento de TI	Programado
25	Aquisição de 50 fones de ouvido c/ microfone	x			Departamento de TI	Programado
26	Aquisição 30 suporte para apoio notebook	x			Departamento de TI	Programado
27	Aquisição 20 adaptadores USB-C para VGA	x			Departamento de TI	Programado

28	Aquisição equipamento Jabra para otimizar áudio em reuniões com até 06 pessoas.	x			Departamento de TI	Programado
29	Aquisição de 10 Webcams para uso Computadores Desktop	x			Departamento de TI	Programado
30	Aquisição de 30 mouses sem fio	x			Departamento de TI	Programado
31	Aquisição de 10 aparelhos telefone IP	x			Departamento de TI	Programado
32	Aquisição de 20 monitores	x			Departamento de TI	Programado
33	Aquisição Monitor/TV 60” para visualização Câmeras Recepção Térreo.	x			Departamento de TI	Programado
34	Adquirir licenças de software definido no estudo de uso de tecnologia com Inteligência Artificial			x	Departamento de TI	Programado
35	Participação da equipe de TI em cursos de capacitação definidos no planejamento de 2024	x	x	x	Departamento de TI	Programado

13 REALIZAÇÕES DOS ANOS ANTERIORES

2022-2023
Análise de Requisitos e Desenvolvimento primeira fase E-PROC (Sistema de Processo Eletrônico da Fiscalização)
Aquisição de 10 notebooks
Realizada troca do sistema de câmeras de monitoramento do prédio sede
Atualizada Política de Backup e aprovada pela Portaria 096/2022
Realizada segmentação da rede em VLANs melhorando a segurança da rede.
Realizada migração redes Wi-fi prédio Sede para nova console Unifi, facilitando gerenciamento e utilização com mesma rede em todo prédio.
Implantação do Softphone para Administrativos e Fiscais possibilitando atendimento e realização de chamadas telefônicas de qualquer local através do notebook.
Implantada Plataforma de Gerenciamento dos Atendimentos WhatsApp concentrando atendimentos e operadores em um único local com gerenciamento e todo histórico das conversas acessível pelas coordenações.
Capacitação da equipe interna de TI para criação, manutenção e utilização dos painéis BI.
Continuidade Projeto de Implantação dos painéis BI com novos painéis para Financeiro, Inadimplência, inclusão de painéis para Depto de Governança e início painéis do Depto. de Tecnologia da Informação. Atualmente temos 09 Painéis Depto. Registro e Relacionamento; 07 painéis Depto. Fiscalização. 11 painéis Depto Financeiro; 07 painéis sobre Inadimplência e 04 painéis Depto. Governança. Totalizando 38 painéis que auxiliam na Gestão.
Atualização de todos os servidores para versão Windows Server 2016 com suas atualizações aplicadas mensalmente.

Integração base de dados cadastral e dos responsáveis técnicos do CRCSC com SEFAZ-SC, totalmente funcional e automatizada.
Integração base de dados cadastral e também dos responsáveis técnicos do CRCSC com SEFAZ-PMF com envio de arquivos semanais gerados pelo CRCSC e carregados na base de dados da Prefeitura Municipal de Florianópolis.
Implantação do sistema SEI com cadastro de todas as unidades organizacionais e usuários para todos os empregados.
Início da utilização do E-PROC (Sistema de Processo Eletrônico da Fiscalização) em produção com processos já iniciando de forma eletrônica; temos atualmente 126 processos ativos tramitando no novo sistema.
Análise de Requisitos e Desenvolvimento segunda fase E-PROC (Sistema de Processo Eletrônico da Fiscalização) que são os Recursos; primeiros testes realizados em dezembro de 2023.
Aquisição de 15 novos notebooks para substituição dos equipamentos atuais dos Fiscais.
Aquisição de 01 servidor de arquivos NAS aumentando segurança dos dados e agilizando as rotinas de backup.
Aquisição de 03 Scanners e 03 Projetores para substituição dos equipamentos mais antigos.

O Plano Diretor de Tecnologia da Informação Biênio 2022-2023 teve grande importância nos avanços do Departamento de Tecnologia da Informação. Conforme demonstrado acima, tivemos melhorias na área de segurança com troca do sistema de câmeras, segmentação da rede local em VLANs e troca das antenas e sistema Wi-fi, assim como aquisições de hardwares e licenças de suítes profissionais de aplicativos de escritório para todos os usuários.

Também tivemos avanços importantes nos convênios com SEFAZ-SC e Prefeitura Municipal de Florianópolis. O primeiro está inclusive totalmente automatizado, com dados cadastrais e também de responsabilidade técnica, agilizando o atendimento aos profissionais da contabilidade.

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 auxiliará os departamentos nesse processo.

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 TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO (CTSI)

2024	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

2025	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 (PSI)

maio/2024

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 institucionais, 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 no site do CRCSC em Governança > Lei Geral de Proteção de Dados (LGPD) > Políticas e termos relacionados à estruturação interna em atendimento LGPD.

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 20__.

Nome:
Matrícula:
Unidade Organizacional:

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