CRA-SC
Conselho Regional de Administração de Santa Catarina

Conselho Regional de Administração de Santa Catarina

Fiscalizar, valorizar e promover o exercício do profissional de Administração, contribuindo com o desenvolvimento do país.

Avenida Prefeito Osmar Cunha, 260 - 8º andar Edifício Royal Business Center - Bairro Centro - Florianópolis-SC - CEP 88015-100
Telefone: 0800 000 1253 - www.crasc.org.br

RESOLUÇÃO NORMATIVA CRA-SC Nº 547 DE 26 DE ABRIL DE 2024

Aprova a Política de Segurança da Informação (PSI) do Conselho Regional de Administração de Santa Catarina e dá outras providências.

O **PRESIDENTE DO CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SANTA CATARINA - CRA-SC**, no uso de suas atribuições que lhe são conferidas pela Lei nº 4.769, de 09 de setembro de 1965, regulamentada pelo Decreto nº 61.934, de 22 de dezembro de 1967, e o Regimento Interno do CRA-SC, aprovado pela Resolução Normativa CFA Nº 592 de 17 de dezembro de 2020, e

CONSIDERANDO a Lei n.º 13.709 (Lei Geral de Proteção de Dados Pessoais – LGPD), de 14 de agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural";

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico e não digital controlado, eficiente e seguro, de forma a oferecer todas as informações necessárias à sociedade, com integridade, confidencialidade e disponibilidade;

CONSIDERANDO a Instrução Normativa n.º 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO a Deliberação da Plenária em sessão ordinária nº 1011, realizada no dia 25 de abril de 2024;

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação (PSI) no âmbito do Conselho Regional de Administração de Santa Catarina, nos termos do Anexo I desta Resolução, e dar outras providências.

Art. 2º Esta Política de Segurança da Informação aplica-se a todos os empregados, estagiários, prestadores de serviços, conselheiros, representantes regionais, membros de câmaras e núcleos e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRA-SC e que tenham acesso a qualquer meio de informação e 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.

Parágrafo único. A íntegra da Política de Segurança da Informação será disponibilizada no Portal da Transparência do CRA-SC.

Art. 3º Esta Resolução Normativa entra em vigor na data da sua assinatura, revogando-se as disposições em contrário.

Adm. Djalma Henrique Hack
Presidente
CRA-SC nº 4889

Documento assinado eletronicamente por **Adm. Djalma Henrique Hack**, **Presidente**, em 26/04/2024, às 17:11, conforme horário oficial de Brasília.

A autenticidade deste documento pode ser conferida no site sei.cfa.org.br/conferir, informando o código verificador **2585115** e o código CRC **6ABB64A5**.

ANEXO I À RESOLUÇÃO NORMATIVA CRA-SC Nº 547 DE 26 DE ABRIL DE 2024

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CRA-SC

CAPÍTULO I - INTRODUÇÃO

1.1 Como recurso de mitigar riscos relacionados à Segurança da Informação, fornecer uma camada adicional de proteção aos dados sensíveis em posse do Conselho Regional de Administração de Santa Catarina (CRA-SC) e garantir que seus ativos sejam protegidos de acordo com sua importância estratégica, a presente política contém um conjunto de padrões, normas e diretrizes que seus destinatários devem seguir, adotando as medidas técnicas de segurança e assim cumprindo a Lei Geral de Proteção de Dados.

CAPÍTULO II - DA ABRANGÊNCIA

2.1 Esta Política de Segurança da Informação aplica-se a todos os empregados, estagiários, prestadores de serviços, conselheiros, representantes regionais, membros de câmaras e núcleos e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRA-SC e que tenham acesso a qualquer meio de informação e 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. Desta forma, é dever de todos, observar as normas e diretrizes em qualquer operação que possa impactar na segurança das informações do Conselho.

2.1.1 Os destinatários devem ter ciência:
- **a.** Das ameaças e preocupações relativas à segurança da informação e;
- **b.** De suas responsabilidades e obrigações no âmbito desta Política.

2.2 Todos devem difundir e exigir o cumprimento desta Política e da legislação vigente acerca do tema.

2.3 É de responsabilidade da Comissão de Gestão da LGPD estabelecer processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os destinatários, de acordo com o seu relacionamento e atribuições no CRA-SC.

2.4 A íntegra da Política de Segurança da Informação será disponibilizada no Portal da Transparência do CRA-SC.

CAPÍTULO III - DO OBJETIVO

3.1 Esta política tem por objetivo 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 no âmbito do Conselho Regional de Administração de Santa Catarina, de forma a garantir os princípios da Segurança da Informação, quais sejam:

a. Confidencialidade: Diz respeito ao caráter das informações ao ponto que apenas quem tem o direito de acesso àqueles dados poderá utilizá-lo, ou seja, deve-se garantir que as informações sejam acessadas apenas por aqueles expressamente autorizados.
b. Disponibilidade: Deve-se garantir que os usuários, quando devidamente autorizados, tenham acesso às informações sempre que necessário.
c. Integridade: Deve-se garantir que a informação esteja completa, legível e que não tenha sido modificada de maneira não autorizada durante o seu ciclo de vida.

3.2 Como complemento desta Política de Segurança da Informação, estão relacionados os seguintes documentos:

a. Manual de Conduta do Conselho Regional de Administração de Santa Catarina;
b. Termo de Confidencialidade e Sigilo;
c. Termo de Responsabilidade de Segurança da Informação.

CAPÍTULO IV - DAS DIRETRIZES

4.1 O cumprimento desta Política e de suas normas de procedimentos complementares deve ser avaliado periodicamente por meio de verificações de conformidade, realizadas pela própria Comissão Especial de Gestão da LGPD.

4.2 O CRA-SC, além das diretrizes estabelecidas nesta política, deve também se orientar pelas melhores práticas e procedimentos de segurança da informação recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões relacionados à segurança da informação.

CAPÍTULO V - DA GESTÃO DE ATIVOS DE INFORMAÇÃO

5.1 Os ativos de informação devem:

a. Ser inventariados e protegidos;
b. Ter identificados os seus proprietários e custodiantes;
c. Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
d. Ter a sua entrada e saída nas dependências do Conselho autorizadas e registradas por autoridade competente;
e. Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;
f. Ser regulamentados por norma de procedimentos específica quanto a sua utilização; e
g. Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

5.2 E, além disso:

a. O CRA-SC deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor, bem como as diretrizes do CFA.
b. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.
c. Os sistemas de informação e as aplicações de uso do Conselho devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.
d. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite do Termo de Responsabilidade de Segurança da Informação.
e. Os ativos de informação devem possuir mecanismos que permitam a auditoria dos eventos de acesso e alteração dos registros.

CAPÍTULO VI - DA GESTÃO DE RISCOS E INCIDENTES

6.1 A Comissão de Gestão da LGPD deve estabelecer mecanismos de Gestão de Riscos de Segurança da Informação que possibilitem identificar ameaças e reduzir vulnerabilidades dos ativos de informação, assim como reduzir os impactos de eventuais incidentes.

6.2 O Conselho estabelecerá as práticas e responsabilidades sobre a gestão de incidentes de segurança da informação e violação de dados pessoais por meio do Plano de Resposta a Incidentes.

6.3 A gestão de incidentes de segurança da informação deverá ser realizada pela Comissão de Gestão da LGPD, por meio de processo formalizado, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança, conforme competências previstas em portaria específica.

CAPÍTULO VII - DO USO DOS RECURSOS DE TECNOLOGIA

7.1 São regras de uso do e-mail corporativo:

a. O usuário é o único responsável pelo conteúdo das transmissões feitas através do e-mail a partir de sua senha ou conta. O usuário não deverá obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço.
b. Não deverão ser abertos arquivos ou executados programas anexados aos emails sem antes verificá-los com um antivírus.
c. Evite enviar anexos desnecessários e grandes por e-mail. Quando necessário, compacte os arquivos e verifique se estão livres de vírus antes de enviar.
d. As mensagens de e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu destinatário. É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela.
e. Respeite a confidencialidade das informações do Conselho. Não compartilhe dados sensíveis ou informações privilegiadas por e-mail, a menos que seja autorizado expressamente pelo Superior Imediato.
f. Mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por vários usuários.
g. Sempre que se ausentar, o usuário deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal.
h. É proibido aos administradores de rede ou e-mail ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte.
i. Não devem ser transmitidos quaisquer materiais ilegais ou, de qualquer forma, censuráveis através do serviço de e-mail. O usuário deve cumprir todas as políticas e diretrizes da empresa relacionadas ao uso do e-mail corporativo. Isso inclui políticas de segurança cibernética, uso aceitável de tecnologia da informação e conformidade regulatória.
j. Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis.
k. Não devem ser transmitidas mensagens não-solicitadas, conhecidas como spam ou junk mail, correntes, ou distribuição em massa de mensagens não solicitadas. Evite encaminhar

correntes, piadas ou conteúdo não relacionado ao ambiente profissional.

l. Responda aos e-mails dentro de um prazo razoável, geralmente dentro de 24 horas úteis. Se não puder fornecer uma resposta imediata, informe o remetente sobre quando eles podem esperar uma resposta mais detalhada.

m. Mantenha sua caixa de entrada organizada, arquivando ou excluindo e-mails irrelevantes e mantendo apenas os necessários para referência futura.

7.2 São regras de uso do telefone (VoIP):

a. O telefone (VoIP e móvel) deve ser usado apenas para propósitos relacionados com os assuntos do Conselho (ex.: para comunicar-se com profissionais e empresas registradas, fornecedores e parceiros conveniados).

b. Recomendamos que o colaborador certifique-se de que não está sendo ouvido por terceiros durante o uso do telefone, quando de discussão de assuntos confidenciais, pois pode gerar exposição de segurança.

c. É dever do usuário estar ciente das políticas e normas do CRA-SC relacionadas ao uso do telefone VoIP. Cumpra todas as diretrizes estabelecidas pelo Conselho para garantir um uso adequado da ferramenta.

d. Mantenha um tom cortês, profissional e respeitoso durante todas as chamadas realizadas através do telefone VoIP, independentemente do destinatário da ligação.

e. Evite fazer ligações através do telefone VoIP fora do horário de expediente, a menos que seja absolutamente necessário e previamente autorizado pelo Superior Imediato.

f. Não compartilhe informações confidenciais ou sensíveis durante chamadas pelo telefone VoIP, especialmente se estiver em um ambiente público ou compartilhando a linha com outras pessoas.

g. Utilize o telefone VoIP de forma consciente e responsável, evitando fazer ligações desnecessárias ou prolongadas que possam impactar negativamente na produtividade.

h. Certifique-se de que o ambiente em que você está realizando a chamada pelo telefone VoIP seja adequado para uma boa qualidade de áudio. Evite ruídos e interrupções que possam prejudicar a comunicação.

i. Esteja aberto ao feedback sobre suas habilidades de comunicação pelo telefone VoIP e utilize-o para aprimorar suas técnicas de comunicação e melhorar a eficácia das chamadas.

j. Reporte qualquer problema técnico ou dificuldade de uso do telefone VoIP ao departamento de TI ou ao suporte técnico da empresa para que seja providenciada assistência adequada.

7.3 São regras de uso da Internet:

a. Alguns sites (páginas da Internet) contêm ou distribuem materiais que não são apropriados para um ambiente de trabalho. Os colaboradores não devem acessar tais sites, ou ainda, distribuir ou obter material similar através da Internet. Os acessos podem estar sendo monitorados a qualquer tempo.

b. Evite acessar sites suspeitos ou não seguros que possam comprometer a segurança dos dados do Conselho. Não compartilhe informações confidenciais ou sensíveis por meio de canais não seguros.

c. Não é permitido o uso de compartilhadores de informações como redes Peer-to-Peer, também conhecidas como redes P2P (eDonkey, eMule, Redes Torrent, etc) dentro do Conselho.

d. Não é permitido o download de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

e. O acesso a redes sociais e outras plataformas de mídia social deve ser limitado ao estritamente necessário para fins profissionais, como parte de uma estratégia de marketing digital, por exemplo. O uso pessoal de redes sociais deve ser evitado durante o horário de trabalho, exceto em casos específicos permitidos pela política do CRA-SC.

f. Seguem exemplos de tipos de sites proibidos:

I. Sites que contenham imagens pornográficas ou materiais relacionados.

II. Sites que contenham atividades ilegais.

III. Sites que contenham intolerância por outros.

IV. Sites de redes sociais (existem exceções para alguns setores).

7.4 São regras de uso da rede corporativa (VPN):

a. O acesso à rede corporativa deve ser concedido apenas aos colaboradores autorizados pelo Conselho. Não compartilhe suas credenciais de acesso com terceiros e reporte imediatamente qualquer suspeita de acesso não autorizado.
b. Para assegurar o backup dos dados, os arquivos relacionados às atividades profissionais devem ser salvos na rede corporativa (cada Setor possui pasta na rede) e não em pastas do usuário do computador. Os arquivos a serem transferidos entre os colaboradores devem ser salvos na pasta “Publico”. Esta pasta, assim como todos os recursos de tecnologia, somente deve ser utilizada para fins estritamente profissionais, sendo o conteúdo, mensalmente, excluído pela TI.
c. A utilização de portas USB e as mídias removíveis são restritas e dependem de autorização dos coordenadores com o conhecimento da TI.
d. É proibida a utilização da rede corporativa para o armazenamento de arquivos de áudio, imagens ou vídeos de uso pessoal.
e. Mantenha a segurança da rede como prioridade, seguindo todas as políticas e diretrizes de segurança estabelecidas pelo CRA-SC. Isso inclui a utilização de firewalls, antivírus, e outras medidas de proteção de dados que serão aplicadas pela TI do Conselho. Em caso de mal funcionamento de algum destes aplicativos, o usuário deverá reportar imediatamente ao suporte de tecnologia.
f. Evite o uso excessivo de largura de banda e recursos da rede, como transferências de arquivos grandes, streaming de vídeo em alta definição ou downloads desnecessários que possam impactar negativamente no desempenho da rede para outros usuários.
g. Reporte imediatamente qualquer incidente de segurança, como tentativas de phishing, malware ou acessos não autorizados, ao departamento de TI ou ao responsável pela segurança da informação do Conselho.
h. O TI deverá realizar, regularmente, backups dos dados armazenados na rede corporativa, garantindo a disponibilidade e integridade dos dados em caso de falhas de hardware ou incidentes de segurança.
i. É também dever do TI, manter todos os softwares e sistemas operacionais utilizados para acessar a rede corporativa atualizados com as últimas correções de segurança e patches disponíveis.

7.5 São regras de uso de senhas:

a. Todos são responsáveis por todos os atos executados com seu login (usuário), que é único e requer senha exclusiva para identificação/autenticação no acesso à Informação e aos recursos de tecnologia.
b. Todos devem assegurar a confidencialidade de sua senha de acesso, ela não pode ser compartilhada, sendo de uso pessoal, intransferível e deverá ser trocada no primeiro acesso.
c. Sempre que possível, ative a autenticação multifatorial (MFA) ou autenticação de dois fatores, para adicionar uma camada extra de segurança. Isso geralmente requer um código enviado para o seu celular ou e-mail antes de permitir o acesso.
d. Evite anotar suas senhas em locais físicos, como post-its ou cadernos. Utilize um gerenciador de senhas confiável para armazenar e proteger suas credenciais de forma segura.

e. A senha é o meio de validação de acessos a recursos e serviços, portanto representa a assinatura digital do colaborador. Sendo assim, recomenda-se que cada colaborador coloque em práticas cuidados básico na proteção deste recurso:
I. Manter a confidencialidade.
II. Não devem ser óbvias, nem derivadas de dados pessoais.
III. Devem ter no mínimo 8 (oito) caracteres.
IV. Devem conter pelo menos 1 (um) caractere alfabético.
V. Devem conter pelo menos 1 (um) caractere numérico.

VI. Devem conter pelo menos 1 (um) caractere especial (! @ # $ % & *).
VII. Não devem conter mais de 3 (três) caracteres consecutivos idênticos à senha anterior.

7.6 São regras de proteção contra vírus e ataques:

a. O vírus de computador é um programa desenvolvido para causar perda ou alteração de dados do computador. Todo equipamento deve ter um programa antivírus instalado, sendo os softwares antivírus atualizados diariamente de forma automática e obrigatoriamente.
b. O colaborador deve efetuar regularmente a busca por vírus em seu computador. Caso seja encontrado vírus, o mesmo deverá consultar o TI do Conselho para obter orientações.
c. Caso o colaborador receba algum e-mail alertando sobre vírus, não deverá passá-lo a outras pessoas, pois a maioria desses alertas é falso. Permanecendo a dúvida, deverá entrar em contato com o TI do Conselho para maiores explicações.

7.7 Da aquisição de Software e Direitos Autorais: A maioria das informações e softwares que estão disponíveis em domínio público (incluindo a Internet) está protegida por leis de Propriedade Intelectual, portanto:

a. Softwares só podem ser instalados com prévia aprovação da autoridade competente. Quando tal ação representar obrigação onerosa e formal ao Conselho, é obrigatória a observância ao devido processo de contratação.
b. A aquisição de software deve estar em conformidade com todas as leis, regulamentos e políticas aplicáveis, incluindo leis de licitação e aquisição de bens e é essencial identificar e definir claramente as necessidades e requisitos do software, incluindo funcionalidades, compatibilidade, segurança e suporte técnico.
c. Ao adquirir um software, deve-se ler e compreender todas as restrições dos direitos autorais do software. Caso o CRA-SC não possa cumprir com as condições estipuladas, não deve ser feito download e não deve ser utilizado o material.
d. O colaborador deverá garantir que cumpre com os requerimentos ou limitações requeridos pelo software (por exemplo, não pode ser utilizado para fins comerciais, não cobrar de outros o uso do software, etc.).

7.8 Da diretriz de tela limpa: Computadores, notebooks e smartphones devem estar protegidos por senha quando não estiverem sendo assistidos.

7.9 Da diretriz de mesa limpa: A política de mesa limpa consiste em não deixar informações confidenciais ou bens do Conselho sem a devida proteção, acessíveis a outras pessoas, quando o colaborador estiver fora do seu local de trabalho. Incluem-se nesta política: papéis, Pen-Drives, CDs ou quaisquer outros tipos de mídias removíveis. São regras de mesa limpa:

a. Ao final do dia de trabalho, computadores portáteis deverão ser guardados em um local seguro ou levados com o seu responsável.
b. Informações confidenciais, quando impressas, devem ser imediatamente retiradas da impressora e trituradas, quando cabível.
c. Não é permitida alimentação, bebida e fumo próximo aos equipamentos.

7.10 Da proteção do patrimônio: Integram o patrimônio físico e intelectual do Conselho, seus imóveis, instalações, equipamentos, estoques, valores, produtos, tecnologia, estratégia de negócio, informações, pesquisas e dados que devem ser protegidos pelos conselheiros e colaboradores, não podendo os mesmos serem utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, seja para que fim for. Não poderão ser utilizados equipamentos ou outros recursos do CRA-SC para fins particulares, salvo se previamente autorizados pelo Superior Imediato. Não podendo ser aprovado caso:
I. Interferir no trabalho do colaborador.
II. Interferir ou concorrer com o negócio do Conselho.
III. Fornecer informação sobre, ou lista de colaboradores a outros.

IV. Envolver solicitação não relacionada aos assuntos do Conselho.
V. Envolver custo adicional para o CRA-SC.

7.11 Da utilização de assinatura digital: o Conselho deve disponibilizar 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.

7.12 Todas as regras e diretrizes aplicam-se, naquilo que couber, ao regime de trabalho híbrido.

CAPÍTULO VIII - DOS CONTROLES DE ACESSOS

8.1 Deverão ser adotadas medidas de proteção para evitar que usuários dos ativos de Tecnologia da Informação tenham permissão para instalar, remover, modificar, criar ou desenvolver softwares sem a devida autorização. Para isso:

a. Devem ser implementados controles de perfis, permissões e procedimentos necessários para a salvaguarda dos ativos de informação do CRA-SC.
b. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.
c. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.
d. Os usuários do CRA-SC são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e certificado digital.
e. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.
f. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.
g. Fica a cargo do Coordenador de cada área definir as permissões de acesso dos usuários às informações de cada sistema, automatizados ou não.
h. Sempre que houver mudança nas atribuições de determinado usuário, as suas permissões de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento ou bloqueados em caso de afastamento.
i. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:
    a. Ao acesso às suas bases de dados;
    b. À extração, carga e transformação de dados.
j. Os sistemas estruturantes devem possuir mecanismos automáticos para:
    a. Revogar as concessões e desativar as contas de acesso usuário nos casos de exoneração, demissão, aposentadoria e falecimento do usuário;
    b. Bloquear as contas de acesso do usuário nos casos de licença, afastamento, cessão e disponibilidade do usuário.

8.2 O controle de usuários dos sistemas é de responsabilidade do TI do CRA-SC, após notificação do RH em conjunto com o Coordenador da área.

CAPÍTULO IX - DA RELAÇÃO COM FORNECEDORES

9.1 Os acordos com terceiros que possuam algum relacionamento com ativos de informação do CRA-SC devem observar as disposições e normas da PSI do CRA-SC.

CAPÍTULO X - DAS DISPOSIÇÕES FINAIS

10.1 A atualização desta Política e demais documentos relacionados é de responsabilidade da Comissão Especial de Gestão da LGPD, devendo submeter à aprovação da autoridade competente, e deve prever a conformidade com as mudanças e inovações legais e institucionais, acompanhando as alterações estratégicas de negócio.

10.2 A Comissão Especial de Gestão da LGPD poderá propor a publicação de políticas adicionais e/ou atualização, conforme consideradas necessárias ou apropriadas.

10.3 A inobservância dos dispositivos constantes nesta Política de Segurança da Informação ou em outras políticas e procedimentos internos é passível de apuração e aplicação das sanções disciplinares cabíveis, sem prejuízo do disposto no Manual de Conduta, respeitando-se o Procedimento Administrativo Disciplinar do CRA-SC, o Código de Ética da Profissão e/ou outras legislações aplicáveis para cada caso.

ANEXO II À RESOLUÇÃO NORMATIVA CRA-SC Nº 547 DE 26 DE ABRIL DE 2024

TERMO DE RESPONSABILIDADE DE SEGURANÇA DA INFORMAÇÃO

Pelo presente termo, eu, _____, declaro ter conhecimento da Política de Segurança da Informação do Conselho Regional de Administração de SC (CRA-SC), disponível para consulta no Portal da Transparência do Conselho.

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

Estou ciente, ainda, de que serei responsável pelo dano que possa causar em caso de descumprimento da Política de Segurança da Informação do CRA-SC.

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

Nome:
CPF: