PORTARIA CRC SP N.º 027/2021 DE 14/10/2021

APROVA DOCUMENTOS DE IMPLANTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD NO ÂMBITO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO

O Presidente do **CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DE SÃO PAULO**, no uso de suas atribuições que lhe são conferidas pelos incisos XVII e XXIV do artigo 18 do Regimento Interno, aprovado pela Resolução CRC SP nº 1.093/11 de 03.10.2011;

CONSIDERANDO que as ações a serem desenvolvidas pelo CRCSP são estruturadas em programas, atividades, projetos, metas e ações, inseridos no Plano de Trabalho, de forma a contribuir para o alcance dos Objetivos Estratégicos,

CONSIDERANDO a necessidade de atender às recomendações do Tribunal de Contas da União (TCU), no que diz respeito ao aprimoramento institucional de governança;

CONSIDERANDO a necessidade da implantação da Lei Nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados – LGPD no âmbito do CRCSP,

RESOLVE:

Artigo 1º. Aprova as Condições Gerais de Uso dos Serviços Online do CRCSP;

Artigo 2º. Aprova a Política de Segurança da Informação do CRCSP;

Artigo 3º. Aprova a Política de Controle de Acesso à Rede e Sistemas Informatizados do CRCSP;

Artigo 4º. Aprova a Política Interna de Proteção de Dados do CRCSP;

Artigo 5º. Aprova a Política de Desenvolvimento de Manutenção de Sistemas do CRCSP;

Artigo 6º. Aprova a Política de Continuidade de Negócios de Tecnologia da Informação do CRCSP;

Artigo 7º. Aprova a Política de Impressão do CRCSP;

São Paulo, 14 de outubro de 2021.

Contador JOSÉ DONIZETE VALENTINA
Presidente


Política de
Segurança
da
Informação

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Equipe Técnica

Cláudio Rafael Bifi - **Diretor Executivo**

Domingos Sávio Mota – **Diretor de Tecnologia e Infraestrutura**

Ronaldo César da Silva - **Gerente do Departamento de Tecnologia da Informação**

Cláudio Molina Paes Rosa – **Coordenador de Sistemas do Departamento de Tecnologia da Informação**

Alessandro de Melo Beserra – **Coordenador de Redes e Segurança do Departamento de Tecnologia da Informação**

Política de Segurança da Informação

(Versão 11.0)

REVISÕES		
DATA	**AUTOR**	**VERSÃO**
20/09/2017	Claudio Molina Paes Rosa	7.0
01/03/2018	Claudio Molina Paes Rosa	7.1
12/09/2018	Claudio Molina Paes Rosa	7.2
07/03/2019	Claudio Molina Paes Rosa	8.0
08/05/2019	Claudio Molina Paes Rosa	9.1
27/09/2019	Claudio Molina Paes Rosa	9.2
05/03/2020	Claudio Molina Paes Rosa	9.3
23/12/2020	Claudio Molina Paes Rosa	10.0
23/09/2021	Claudio Molina Paes Rosa	11.0

Sumário

1. DOS MOTIVOS

1.1. Ciente da relevância das informações que trafegam na rede de dados, e os riscos a que estas estão sujeitas diariamente, o Conselho Regional de Contabilidade do Estado de São Paulo - CRC SP passa a implantar a Política de Segurança da Informação no âmbito do CRC SP.

1.2. A utilização de uma política de segurança da informação constitui importante ferramenta para minimizar os riscos enfrentados pela informação, dentre os quais: invasões, furtos, espionagem, vandalismo, sabotagem, perda de informações ou ataques de hackers e infestação vírus.

1.3. Ao CRC SP, através da Gerência de Tecnologia da Informação - TI, é imprescindível regular o uso indevido da rede de computadores, em especial acessos que não se relacionem às funções legais do CRC SP.

1.4. A política de segurança da informação é aplicável à utilização de todas as ferramentas disponibilizadas aos empregados do CRC SP no exercício das suas funções, tais como: correio eletrônico (e-mail), rede mundial de computadores (internet), equipamentos, rede, etc.

1.5. Compreende-se que o acesso à internet e a utilização de e-mails através da rede corporativa do CRC SP, destina-se única e exclusivamente às necessidades do serviço prestado.

1.6. Os serviços prestados pelo CRC SP não podem ser prejudicados, seja pela sobrecarga causada à infraestrutura, em razão do excesso de e-mails contendo arquivos não relacionados às reais funções executadas pelos seus empregados ou mesmo a consulta a sites de diversas naturezas.

1.7. Tal política deverá ser plenamente atendida por todos os usuários de informática no âmbito do CRC SP tais como conselheiros, empregados, assessores, terceirizados, estagiários, aprendizes, colaboradores, usuários da rede visitante (sem fio) do CRC SP, parceiros e/ou empresas contratadas pelo CRC SP, sendo passível da aplicação das penalidades administrativas correlatas, observadas as normas internas para a ampla defesa.

2. DAS SENHAS

2.1. O cadastramento de usuários será feito mediante solicitação do Departamento responsável através de chamado no Help Desk, devendo ser informado o nome completo, a lotação e a matrícula do empregado, sendo obrigatório também a vigência do contrato nos casos de estagiários, menores aprendizes ou prestadores de serviços.

2.2. O usuário cadastrado terá acesso à rede de dados do CRC SP, a um endereço de e-mail corporativo e aos sistemas internos, quando for o caso.

2.3. As contas dos estagiários, menores aprendizes e prestadores de serviço serão configuradas para expiração automática, concomitantemente à vigência do contrato.

2.4. Os nomes de usuários obedecerão um padrão composto pelo primeiro nome, seguido pelas iniciais dos sobrenomes conforme necessário para distinção dos usuários já existentes.

2.5. No 1º acesso, o usuário deverá modificar tais senhas, sendo de livre escolha do usuário, porém altamente recomendável a utilização de senhas fortes preferencialmente com 6 ou mais caracteres, mesclando entre caracteres numéricos e letras maiúsculas

2.6. Deve-se evitar senhas que contenham dados do seu cadastro, iniciais do nome, data de nascimento e outras de fácil dedução

2.7. O usuário é o único e exclusivo responsável pela utilização das suas senhas, inclusive por danos e prejuízos que venham a ser causados em decorrência do seu mau uso.

2.8. Caso o usuário desconfie que terceiros tiveram acesso às suas senhas ou ocorra um comprometimento comprovado de segurança do ambiente de TI, este deverá comunicar imediatamente o Departamento de TI, para o bloqueio de seus acessos e demais instruções.

2.9. Apesar da solicitação automática para alteração das senhas, o Departamento de TI recomenda que o usuário altere sua senha a cada 60 (sessenta) dias ou na periodicidade que entender conveniente. A senha cadastrada terá prazo de validade de 120 (cento e vinte) dias, ao fim do qual o usuário será obrigado a redefinir sua senha.

2.10. As SENHAS SÃO PESSOAIS E INTRANSFERÍVEIS e não devem ser divulgadas a terceiros, mesmo que sejam empregados do CRC SP.

2.11. Durante o período de férias e/ou licença do usuário, as senhas serão suspensas.

3. DO CORREIO ELETRÔNICO (E-MAIL)

3.1. Todo usuário do CRC SP possui um endereço e caixa de e-mail corporativo, cujo domínio "@crcsp.org.br" é de propriedade exclusiva do CRC SP, não podendo ser utilizado para assuntos de ordem pessoal.

3.2. Todas as mensagens distribuídas pelo domínio "@crcsp.org.br", ainda que com conteúdo particular, são de propriedade do CRC SP.

3.3. A identificação do usuário será o nome cadastrado pelo Departamento de TI, seguido do domínio "@crcsp.org.br" (usuario@crcsp.org.br).

3.4. O envio e recebimento de e-mails são restritos ao ambiente interno do CRC SP, salvo os casos cujas atribuições das funções e trabalhos executados necessitem do envio e recebimento de mensagens externas.

3.5. A política de segurança da informação tem como propósito, assegurar o uso apropriado e seguro do sistema de e-mails no âmbito do CRC SP, assim impossibilitando o tráfego de conteúdo sigiloso e/ou incompatível com as reais funções executadas no CRC SP.

3.6. Com a utilização do domínio "@crcsp.org.br", o usuário não deve manter qualquer expectativa de privacidade sobre os e-mails criados, armazenados, enviados ou recebidos.

3.7. O usuário fica ciente que as mensagens do domínio "@crcsp.org.br" são monitoradas.

3.8. Na utilização do e-mail corporativo "@crcsp.org.br", fica expressamente proibido enviar, encaminhar ou responder e-mails com:

a) conteúdo pornográfico, obsceno ou sexual;
b) comentários discriminatórios, difamatórios ou ofensivos;
c) jogos, arquivos de áudio ou vídeo.
d) spam, phishing ou correntes de qualquer natureza;
e) mensagens copiadas ou anexadas de outro usuário sem a permissão expressa daquele.

3.9. Fica ainda proibido forjar ou tentar forjar mensagens de e-mail, disfarçar ou tentar disfarçar sua identidade quando enviando um e-mail.

3.10. O descumprimento das citadas regras, possibilitará ao CRC SP o direito de tomar medidas disciplinares cabíveis, incluindo ação judicial, conforme o caso.

3.11. Caso receba algum e-mail contendo arquivos dessa natureza, este deverá, imediatamente, ser RETRANSMITIDO ao Departamento de TI (informatica@crcsp.org.br).

3.12. Todo e-mail enviado para fora do CRC SP, deverá ser finalizado com a seguinte comunicação de isenção (disclaimer):

"Esta mensagem é direcionada apenas aos endereços constantes no cabeçalho inicial. Se você não está listado nos endereços constantes no cabeçalho, pedimos-lhe que desconsidere completamente o conteúdo dessa mensagem. As informações contidas nesta mensagem são CONFIDENCIAIS. A divulgação, distribuição, reprodução ou qualquer forma de utilização do teor deste documento depende de autorização do emissor, sujeitando-se o infrator às sanções legais. O emissor desta mensagem utiliza o recurso somente no exercício do seu trabalho ou em razão dele, eximindo-se o empregador de qualquer responsabilidade por utilização indevida ou pessoal. Caso esta comunicação tenha sido recebida por engano, favor avisar imediatamente, respondendo esta mensagem. Apesar do CRC SP tomar todas as precauções razoáveis para assegurar que nenhum vírus esteja presente nesse e-mail, o CRC SP não poderá aceitar a responsabilidade por quaisquer perdas ou danos causados por esse e-mail ou por seus anexos.".

3.13. As regras acima citadas também se aplicam ao endereço eletrônico dos departamentos do CRC SP.

4. DA REDE MUNDIAL DE COMPUTADORES (INTERNET)

4.1. A utilização da internet no âmbito do CRC SP é restrita, tendo acesso somente a sites com extensão “. org.br”, “. gov.br”, além dos sites necessários para a execução dos trabalhos e movimentação financeira particular dos usuários.

4.2. O site de pesquisa “Google” é liberado exclusivamente para pesquisas relacionadas ao trabalho executado. Qualquer pesquisa com outro propósito constitui conduta passível da aplicação de penalidade administrativa.

4.3. Mediante solicitação do titular do departamento, com ciência da respectiva Diretoria, e após análise do Departamento de TI, outros sites poderão ser autorizados.

4.4. A critério exclusivo do Departamento de TI, o acesso a qualquer site que ameace a política de segurança da informação ou que não sejam de interesse diretamente relacionados aos trabalhos executados do CRC SP poderá ser bloqueado, independentemente de autorização anterior ou notificação formal.

4.5. Valer-se de conhecimento técnico para burlar a política de segurança da informação a fim de acessar sites bloqueados pelo Departamento de TI, constitui conduta passível da aplicação de penalidade administrativa.

4.6. O CRC SP veda, expressamente, a utilização da internet para invadir quaisquer sites ou de rede de informações, disseminar vírus ou outras práticas relacionadas ao mal-uso da internet.

4.7. De acordo com as atribuições do cargo e rotinas de trabalho o acesso poderá ser liberado.

4.8. É expressamente proibido ao usuário do CRC SP o acesso a site que vincule matéria relacionada à pornografia, jogos em rede, áudio, vídeo e salas de bate-papo ou qualquer outro que possa vir a prejudicar ou colocar em risco a integridade do CRC SP.

4.9. O acesso à rede BYOD Wi-Fi do CRC SP poderá ser concedido mediante solicitação superior com suas devidas justificativas e autorização da respectiva Diretoria, não sendo recomendado sua utilização na transmissão de streaming.

4.10. É permitido o acesso à rede Wi-Fi “CRC VISITANTES” do CRC SP, onde o usuário, deverá se identificar e concordar com o termo de uso da rede sem fio.

4.11. Os acessos à internet através das redes Wi-Fi possuem as mesmas restrições conforme descriminado no item 4.1.

4.12. Mediante solicitação do titular do departamento, o TI poderá fornecer relatórios mensais dos acessos para permitir o devido controle.

5. DOS EQUIPAMENTOS

5.1. Os equipamentos de informática de propriedade do CRC SP deverão ser utilizados exclusivamente por empregados do CRC SP mediante login, sendo o uso exclusivo para execução de tarefas relacionadas às funções no CRC SP.

5.2. O usuário deverá zelar pela limpeza e conservação dos equipamentos, mantendo-o em perfeitas condições de uso, verificando inclusive os acessórios.

5.3. É expressamente proibido colar adesivos ou fotos, fixar imãs ou colocar sobre os equipamentos objetos que possam danificar o mesmo (vasos, bebidas, líquidos, etc.)

5.4. A instalação de programas é proibida, sob pena de ser responsabilizado, salvo prévia autorização do Departamento de TI.

5.5. A instalação e desinstalação de programas somente poderão ser realizadas pelo Departamento de TI.

5.6. O Departamento de TI não se responsabiliza por material de trabalho mantido localmente nos equipamentos, seja em casos de necessidade da troca ou formatação do equipamento.

5.7. O Departamento de TI não efetua, em hipótese alguma, cópia dos arquivos armazenados no equipamento.

5.8. Somente empregados e pessoas designadas pelo Departamento de TI tem permissão para a abertura física dos equipamentos de informática, aos demais usuários do CRC SP tal prática é expressamente proibida.

5.9. Somente o CRC SP deve garantir o fornecimento e funcionamento dos equipamentos necessários para todo e qualquer tipo de trabalho realizado, dentro ou fora das dependências do CRC SP visando garantir sempre a segurança e integridade das informações, sendo assim, é vedada a utilização de recursos computacionais (hardware e software) de propriedade particular, para a execução de trabalhos inerentes ao CRC SP.

5.10. Somente equipamentos de propriedade do CRC SP, configurados e com softwares de segurança instalados pelo Departamento de TI e atualizados podem acessar a rede cabeada do CRC SP.

5.11. Nos casos de Convênios, Palestrantes e Visitantes, o departamento responsável disponibilizará equipamento para que o usuário externo possa realizar seus trabalhos.

5.12. É proibido aos funcionários do CRC SP, a utilização de recursos computacionais (hardware e software) de propriedade particular, para qualquer fim, nos departamentos do CRC SP.

5.13. É permitido aos funcionários a utilização de Notebooks ou similares, de propriedade particular, dentro das áreas livres (Biblioteca, Saguão e Auditório) e podem sendo de total responsabilidade do funcionário quaisquer atividades desenvolvidas nos referidos equipamentos.

6. DO ACESSO À VPN DO CRC SP

6.1. Por padrão o acesso à VPN do CRC SP é bloqueado, pois podem abrir brechas que venham a comprometer a segurança do nosso ambiente tornando-o vulnerável;

6.2. Para liberação do acesso à VPN do CRC SP, é necessário a abertura de chamado via Help Desk na categoria “Suporte” contendo uma justificativa para a solicitação do acesso;

6.3. Após a liberação do acesso pelo Departamento de TI, o colaborador será contactado para que possa trazer o equipamento ao Departamento de TI pois o mesmo deve ser configurado utilizando-se o perfil do usuário;

6.4. Por questões de segurança, o acesso à VPN só pode ser configurado em equipamentos fornecidos pelo CRC SP, onde é garantido que todas as soluções contra agentes maliciosos (vírus, malwares etc.) estejam atualizadas;

7. DO AMBIENTE DE REDE

7.1. Todo usuário terá direito a diretório de rede exclusivo, salvo por empregados do Departamento de TI, previamente autorizados pelo Gerente de TI.

7.2. A critério exclusivo do TI, tal diretório terá capacidade de armazenamento limitada, podendo ser reduzida sem prévia notificação.

7.3. Diariamente é realizado backup dos arquivos mantidos na rede.

7.4. As regras acima citadas também se aplicam aos diretórios dos departamentos.

8. DOS ARQUIVOS DE FOTOS, VÍDEOS OU MÚSICAS

8.1. A fim de não sobrecarregar a rede, fica proibido o armazenamento de arquivos de fotos, vídeos, músicas e apresentações nos diretórios de rede do usuário e/ou departamento, podendo o Departamento de TI excluir eventuais arquivos sem prévia notificação.

8.2. Os arquivos de fotos, vídeos, músicas e apresentações, podem ser armazenados na máquina do usuário, não sendo de responsabilidade do Departamento de TI a guarda destes arquivos;

8.3. Havendo necessidade de armazenagem em rede, o assunto deverá ser submetido à apreciação do Gerente de TI.

8.4. Os departamentos que possuem ferramentas para realização de backup deste tipo de arquivo, não devem utilizá-los para outros fins que não sejam profissionais.

9. DO USO DAS IMPRESSORAS

9.1. O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra.

9.2. A utilização das impressoras deverá ser estritamente profissional, não sendo permitido usá-las para fins pessoais.

9.3. O usuário deverá valer-se dos recursos das impressoras para utilização de forma econômica.

9.4. Gerência de Tecnologia da Informação poderá a qualquer momento, sem aviso prévio, efetuar auditoria e/ou monitoramento das impressões feitas pelos usuários, assim como limitá-las e/ou restringi-las, sempre em comum acordo com a chefia.

10. DIRETRIZES QUANTO AO USO DE MÍDIAS REMOVÍVEIS E DA PORTA USB

10.1. O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra.

10.2. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modens 3G e os pen drives merecem a atenção. Tal vulnerabilidade não pode ser contida com firewalls ou com programas antivírus já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa.

10.3. Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação da chefia do departamento do solicitante. Para notebooks de gerentes e cargos acima esta liberação é efetuada por padrão.

10.4. Dentro da empresa dê preferência à utilização da rede evitando a utilizando de modem 3G conectado à porta USB do computador, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o funcionário abre a porta para acesso sem qualquer controle.

10.5. Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados.

10.6. É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

10.7. É proibido sem autorização previa o uso de informações de caráter corporativo para o uso pessoal;

10.8. É proibido a cópia para pendrive pessoal, dispositivo de armazenagem, email pessoais, de informações do CRCSP;

10.9. O transporte de informações não públicas por meio de um pendrive sujeita-as a riscos de acesso indevido no caso de perda, roubo ou qualquer outra forma pela qual alguém tenha acesso físico ao dispositivo.

11. DO USO DO WHATSAPP WEB E APLICATIVOS DE ARMAZENAMENTO EM NUVEM (DROPBOX, ONEDRIVE, GOOGLE DRIVE ETC.)

11.1. Por padrão o uso do WhatsApp Web e aplicativos de armazenamento em nuvem como o Dropbox, OneDrive ou Google Drive é bloqueado, pois podem abrir brechas que venham a comprometer a segurança do nosso ambiente tornando-o vulnerável;

11.2. Para liberação do uso destes aplicativos, é necessário a abertura de chamado via Help Desk, além de uma autorização formal assinada pelo Diretor de Tecnologia e Infraestrutura que deverá ser entregue ao Departamento de TI;

11.3. O Departamento de TI não se responsabiliza pelo conteúdo das mensagens e/ou arquivos que venham a ser trocados ou armazenados com o uso destes aplicativos;

11.4. A qualquer momento o Departamento de TI poderá efetuar auditoria e/ou monitoramento do conteúdo trocado ou armazenado no uso destes aplicativos;

12. BOAS PRÁTICAS DE SEGURANÇA PARA NOTEBOOK

12.1. Quando em deslocamentos de carro, coloque o mesmo no porta-malas ou em local não visível.

12.2. Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para Notebook e sim mochilas ou malas discretas.

12.3. Não coloque o notebook em carrinhos de aeroportos ou despache junto à bagagem.

12.4. Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.

12.5. Evite utilizar o notebook em locais públicos.

12.6. Nos hotéis, preferencialmente, guarde o notebook no cofre do seu apartamento.

12.7. Avalie se em pequenas viagens é realmente necessário levar o notebook.

13. DA AUDITORIA E MONITORAMENTO

13.1. Por ocasião da implantação desta política de segurança da informação, a Gerência de Tecnologia da Informação terá acesso irrestrito e ilimitado de todo conteúdo informatizado do CRC SP, dentre os quais diretórios de rede, pastas, arquivos, acessos a sites, e-mail, etc., podendo a qualquer momento, efetuar AUDITORIA e/ou MONITORAMENTO, sem prévio aviso.

13.2. Dada à natureza sigilosa dos procedimentos de auditoria e/ou monitoramento, o empregado designado para sua execução deverá apresentar o resultado exclusivamente ao Gerente de TI, sob pena de responsabilização pelo vazamento de informações.

13.3. O resultado da auditoria e/ou monitoramento que constatar o descumprimento da política de segurança da informática e/ou existência de conteúdo proibido no âmbito do CRC SP será imediatamente encaminhado ao titular do departamento ou respectiva diretoria para adoção dos procedimentos administrativos de praxe.

14. DAS DISPOSIÇÕES GERAIS

14.1. No que tange a Política de Segurança da Informação, são considerados assuntos com conteúdo impróprio:

a) Erótico
b) Nudez
c) Pornografia

d) Pornografia Infantil (Pedofilia)
e) Jogos
f) Racismo
g) Apologia ao Crime
h) Apologia à Violência
i) Apologia à Drogas
j) Ofensa a Religião
k) Relacionamentos
l) Prostituição

14.2. As dúvidas relacionadas à política de segurança da informação serão dirimidas pela Gerência de Tecnologia da Informação, através do e-mail: informatica@crcsp.org.br.

14.3. À legislação acostada à presente política poderão ser adicionadas outras normas correlatas.

14.4. Cabe à Gerência de Tecnologia da Informação adotar os procedimentos necessários para a ampla publicidade desta política e suas atualizações.

14.5. Nas novas contratações de empregados, o Departamento de Recursos Humanos deverá atualizar o contrato de trabalho para que se faça mencionar a presente política.

14.6. Cabe ao Departamento de Recursos Humanos informar as férias, licenças ou desligamento dos usuários, a fim de que a Gerência de Tecnologia da Informação adote as providências para suspensão dos acessos.

14.7. Ao usuário cabe acompanhar a atualização da Política de Segurança da Informação e seu fiel e irrestrito cumprimento.


Condições
Gerais de
Uso dos
Serviços
On Line

Sumário

1. CONDIÇÕES GERAIS E SUA ACEITAÇÃO

- Estas condições gerais ("Condições Gerais") regulamentam o uso dos Serviços On Line ("Serviços On-Line") que o Conselho Regional de Contabilidade do Estado de São Paulo ("CRCSP") disponibiliza gratuitamente aos usuários de Internet através do portal www.crcsp.org.br.
- Para a utilização dos Serviços On Line o usuário do Serviço ("Usuário") deverá aceitar expressa e plenamente, totalmente sem reservas do Usuário, as Condições Gerais na versão publicada pelo CRCSP no momento em que o Usuário acessa os Serviços On Line.
- Desta forma, o Usuário deve ler atentamente as Condições Gerais em cada uma das ocasiões em que se propor a utilizar os Serviços On-Line.

2. OBJETO

- As presentes Condições Gerais regulamentam a prestação dos Serviços On-Line por parte do CRCSP e a utilização dos Serviços On-Line por parte dos Usuários.
- O CRCSP se reserva ao direito de modificar unilateralmente, a qualquer tempo e sem prévio aviso, a apresentação e configuração dos Serviços On-Line, assim como quaisquer das condições requeridas para utilizar os Serviços On-Line.

3. OS SERVIÇOS ON-LINE

- Os Serviços On-Line é um ambiente virtual que possibilita, através dos serviços, agilizar a rotina de trabalho dos profissionais registrados no CRCSP.

4. CONDIÇÕES DE USO DA SENHA

- Cada Usuário do CRCSP, para ter acesso aos serviços oferecidos, deverá ter uma senha, é fornecida pelo CRCSP, que posteriormente, deverá ser modificada pelo usuário, sendo de livre escolha a nova senha.
- A senha é de responsabilidade exclusiva do Usuário e poderá ser alterada tantas vezes quanto desejar através dos Serviços On-Line.
- A SENHA É PESSOAL E INTRANSFERÍVEL e não deve ser divulgada a terceiros pelo por qualquer das partes.
- Caso o Usuário desconfie que terceiros tiveram acesso à sua conta ou senha, deverá imediatamente comunicar o CRCSP para que efetue o bloqueio de seu acesso e a reative em caso de solução.

- É recomendável que o Usuário altere sua senha a cada 03 meses.
- O Usuário é o único e exclusivo responsável pela utilização de sua senha, inclusive por danos e prejuízos que venham a ser causados em decorrência do mau uso.

5. UTILIZAÇÃO DO SERVIÇO SOB A EXCLUSIVA RESPONSABILIDADE DO USUÁRIO

- O Usuário declara, neste ato, que aceita voluntariamente que a utilização dos Serviços On Line, em qualquer caso, é de sua única e exclusiva responsabilidade.
- O Usuário é integralmente responsável pelos equipamentos físicos ("hardware") necessários para conexão à Internet (computador, linha telefônica, modem, etc.) e pelos custos de instalação, conexão, tarifação da linha telefônica, energia elétrica e outros custos inerentes.
- O Usuário assume o compromisso de não empregar qualquer recurso tecnológico, tangível ou intangível, que tenha por objetivo reverter ao CRCSP os custos inerentes à sua própria conexão à Internet, assim como tomar qualquer medida que possa imputar ao CRCSP os custos mencionados no item acima.

6. DAS OBRIGAÇÕES DO USUÁRIO

- O Usuário compromete se a não utilizar os serviços, objeto deste contrato para:
  - Obter informações a respeito de terceiros, em especial endereços de correio eletrônico, sem anuência do titular/Usuário;
  - Não assumir a "personalidade" de outra pessoa, física ou jurídica, incluindo, mas não se limitando a, representante do CRCSP, ou ainda declarar-se ou apresentar-se falsamente como Usuário de alguma entidade ou pessoa notória;
  - Não interferir ou interromper o Serviço, as redes ou os servidores conectados ao Serviços On Line, obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao Serviços On Line ou desobedecer qualquer regra, procedimento, política ou regulamento de redes ou sistemas conectados ao Serviço;
  - Não violar, seja intencionalmente ou não, qualquer norma legal municipal, estadual, nacional ou internacional que seja integrada ao sistema brasileiro;
  - Não obter ou armazenar dados pessoais sobre outros Usuários, inclusive, mas não se limitando, a informações financeiras.
- O CRCSP se reserva ao direito de restringir o acesso do Usuário à sua própria conta e demais serviços prestados mediante o uso do site CRCSP que é gratuitamente disponibilizado.

7. USO DE INFORMAÇÕES DE CADASTRO

- Desde já o Usuário autoriza ao CRCSP o envio de e-mails contendo propaganda do CRCSP ou de seus parceiros para o endereço eletrônico do Usuário. Bem como e mails de caráter técnico ou informativo.
- O Usuário declara ter ciência de que o CRCSP poderá utilizar "COOKIES" ou outros meios análogos de identificação do Usuário.

8. DISPOSIÇÕES GERAIS

- O CRCSP é o único detentor dos direitos de utilização e exploração do domínio "crcsp.org.br", não cedendo ou transferindo ao Usuário quaisquer direitos.
- O Usuário responderá, perante terceiros em geral, pela violação de direitos de propriedade imaterial, incluindo, mas não se limitando, a propriedade intelectual, literária, artística e de propriedade industrial que se referem os privilégios de invenção, marcas de indústria e comércio, desenhos de utilidade e etc, eximindo o CRCSP de quaisquer responsabilidades.
- O CRCSP poderá cooperar com as autoridades policiais e judiciais para localização de indivíduos que possuam Páginas Pessoais (Home Page) com conteúdo ilegal ou duvidoso.

Política de Controle de Acessos

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Equipe Técnica

Cláudio Rafael Bifi - **Diretor Executivo**

Domingos Sávio Mota – **Diretor de Tecnologia e Infraestrutura**

Ronaldo César da Silva - **Gerente do Departamento de Tecnologia da Informação**

Cláudio Molina Paes Rosa – **Coordenador de Sistemas do Departamento de Tecnologia da Informação**

Alessandro de Melo Beserra – **Coordenador de Redes e Segurança do Departamento de Tecnologia da Informação**

Política de Controle de Acessos

(Versão 4.0)

REVISÕES		
DATA	**AUTOR**	**VERSÃO**
20/09/2017	Claudio Molina Paes Rosa	2.0
01/03/2018	Claudio Molina Paes Rosa	2.1
12/09/2018	Claudio Molina Paes Rosa	2.2
07/03/2019	Claudio Molina Paes Rosa	2.4
20/09/2019	Claudio Molina Paes Rosa	3.0
03/03/2020	Claudio Molina Paes Rosa	3.1
23/12/2020	Claudio Molina Paes Rosa	3.2
23/09/2021	Claudio Molina Paes Rosa	4.0

Sumário

1. DOS OBJETIVOS

- Regular a concessão ou revogação de acessos dos usuários aos sistemas e à rede de dados do CRC SP
- Reunir e documentar as práticas adotadas na instituição

2. SOBRE O CONTROLE DE ACESSO

- O controle de acesso, na segurança da informação, é composto dos processos de autenticação, autorização e auditoria. Neste contexto o controle de acesso pode ser entendido como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo). A autenticação identifica quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer, e a auditoria diz o que o usuário fez;

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

- A identificação e autenticação fazem parte de um processo de dois passos que determina quem pode acessar determinado sistema. Durante a identificação o usuário diz ao sistema quem ele é (normalmente através de um nome de usuário). Durante a autenticação a identidade é verificada através de uma senha fornecida pelo usuário;

4. AUTORIZAÇÃO

- A autorização define quais direitos e permissões tem o usuário do sistema. Após o usuário ser autenticado o processo de autorização determina o que ele pode fazer no sistema;

5. NOVOS USUÁRIOS / MUDANÇA DE DEPARTAMENTO

- As solicitações para novas identificações de usuários e alterações de privilégios devem ser feitas pela chefia ao TI através da abertura de chamado no Help Desk. O solicitante deve declarar claramente o acesso requerido e porque são necessárias alterações em seus privilégios e a relação de tais alterações com as atividades exercidas;
- No caso de um novo colaborador ou até mesmo em uma mudança de departamento, é extremamente recomendado que seja informado um usuário de referência para que seja efetuado uma cópia dos acessos. Utilizando-se desse método, podemos garantir que os acessos relativos ao departamento anterior sejam revogados.

6. DESLIGAMENTO DO FUNCIONÁRIO DA EMPRESA

- A Conta do usuário na empresa é desativada, preservando os logs de acessos do funcionário.
- Cabe ao Departamento de Recursos Humanos informar as férias, licenças ou desligamento dos usuários, a fim de que a Gerência de Tecnologia da Informação adote as providências para suspensão dos acessos.

7. ACESSOS

- O acesso a informações rotuladas como públicas e uso interno não é restringido com controles de acesso que discriminam o usuário. Por outro lado, o acesso às informações confidenciais ou restritas será permitido apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pela unidade responsável. Da mesma forma, o acesso a alguns equipamentos de hardware e/ou software especiais (como equipamentos de diagnóstico de rede chamados “sniffers”) deve ser restrito a profissionais competentes, com uso registrado e baseado nas necessidades do órgão;
- Recursos automáticos – Será dado a todos os usuários, automaticamente, o acesso aos serviços básicos como correio eletrônico, aplicações de controle e browser WEB. Estas facilidades básicas irão variar de acordo com os cargos e serão determinadas pela autoridade competente em cada órgão público. Todos os outros recursos dos sistemas serão providos via perfis de trabalho, conforme item 5, ou por uma solicitação especial feita ao proprietário da informação envolvida. A existência de acessos privilegiados, não significa por si só, que um indivíduo esteja autorizado a usar esses privilégios. Se os usuários tiverem quaisquer questões sobre controle de acessos privilegiados, deverão direcionar suas perguntas unidade competente dentro do CRC SP;
- Para cada programa (tela) disponível no SPI (Sistema de Profissionais Inscritos), existe um departamento proprietário que é responsável em conceder ou revogar seus acessos;
- Os usuários do departamento que podem conceder ou revogar os acessos aos programas do SPI que são responsáveis são os gerentes, chefes e coordenadores;
- Os acessos podem ser concedidos ou revogados também à usuários de outros departamentos;
- As concessões ou revogações de acesso aos programas do SPI são feitas através de uma tela específica chamada “Acesso Funcionários”;
- Periodicamente o proprietário do programa deve efetuar uma conferência dos usuários que possuem acesso aos programas cujo seu departamento é responsável;
- Esta periodicidade é definida pelo próprio proprietário baseada em 3 níveis de riscos: baixo, médio e alto, cujos prazos são 365, 180 e 30 dias respectivamente;
- Sempre que houver algum programa cujo prazo de conferência de acessos estiver expirado, o sistema redirecionará o usuário à tela de conferências automaticamente após o login no

sistema e exibirá uma mensagem de alerta, além de enviar e-mail para o TI informando o atraso;

- Os acessos concedidos e/ou revogados no item anterior são devidamente registrados nos logs do sistema;
- Quando houver a necessidade de acessar um módulo cujo responsável não seja o gestor do próprio departamento, o usuário deve solicitar acesso ao responsável direto desse sistema;

8. USUÁRIOS EXTERNOS / TEMPORÁRIOS

- Todos aqueles que não são usuários diretos do CRC SP (contratados, consultores, temporários etc.) têm que solicitar à chefia do departamento em que está lotado, os acessos inerentes ao seu trabalho. Os privilégios destas pessoas deverão ser imediatamente revogados quando da finalização do trabalho temporário. O mesmo deverá ser observado no desligamento antecipado, considerando ainda a responsabilização pelas atividades e atos cometidos durante a sua permanência no CRC SP;

9. SOBRE O SISTEMA GERENCIADOR DE RELATÓRIO

- Os acessos para gerar relatório de até 3.000 registros por mês somente competem a chefia do departamento e ao seu coordenador;
- Somente dois funcionários por departamento tem direito a geração de relatório dos registros;
- Se porventura houver a necessidade de conceder acesso à geração de relatório a outro funcionário, o mesmo deve ser solicitado ao Diretor de TI e Infraestrutura;
- Somente usuários autorizados pela Diretoria de TI e Infraestrutura podem gerar relatório com mais de 3.000 registros por mês;
- O limite de 3.000 registros por mês não é considerado para a geração de arquivos textos (somente e-mail), pelo fato de o e-mail ser criptografado e ser acessível somente pelo Mail News.

10. SOBRE O MAIL NEWS

- Em função do sistema de envio de e-mails Mail News pertencer ao TI, o acesso a ele deve ser solicitado exclusivamente pelo Help Desk.
- A quantidade de e-mails disparados por usuário permitida é controlada pelo TI, sendo o padrão de 10 mil e-mails por dia não acumulativa.
- Para que o limite diário de e-mails disparados seja maior que o pré-definido, é necessário que a solicitação seja feita via abertura de chamado no Help Desk contendo uma justificativa para tal.


Política Interna de Proteção de Dados Pessoais do CRCSP

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Comissão de Implantação da Lei Geral de Proteção de Dados – LGPD do CRCSP

Domingos Sávio Mota - **Coordenador**
Cláudio Rafael Bifi – ***Vice Coordenador***

Membros

Ronaldo César da Silva
Fernando Eugênio do Santos
Gilmar Pires de Simões
Valeria Vanessa de Campos Pinezi
Reginaldo Gomes Ferreira
Clarindo Bibiano de Araújo
Luiz Fernando Lopes
Rosa Maria Pereira
Luciana de Souza Ramos
Elaine Constantino Santos
Guilherme Andreas Campos Del Guerra
Andrea Fernandes dos Santos Guenka

Política Interna de Proteção de Dados Pessoais do CRCSP

(Versão 1.0)

Histórico de Alterações

Data	Versão	Descrição	Autor

Sumário

1. Introdução

Com a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais, foi necessário estabelecer diretrizes para o tratamento interno de dados pessoais no âmbito do CRCSP.

2. Objetivos e Princípios

A Política Interna de Proteção de Dados Pessoais do CRCSP, tem por objetivo orientar a todos os operadores acerca das boas práticas em proteção de dados pessoais, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

Os princípios norteadores da LGPD e desta Política Interna são:

a) **Finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

b) **Adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

c) **Necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

d) **Livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

e) **Qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

f) **Transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

g) **Segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

h) **Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

i) **Não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

j) **Responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3. Responsabilidade e do Tratamento de Dados Pessoais

A responsabilidade pelo correto tratamento dos dados pessoais dentro do CRCSP é compartilhada entre todos aqueles que atuam como operadores, necessitando da cooperação dos envolvidos para o atendimento aos dispositivos legais e segurança dos dados pessoais sob seu controle.

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, conforme disposto no art. 42 e seguintes da LGPD.

O tratamento dos dados pessoais no CRCSP deve seguir os princípios definidos nesta política, devendo ser estritamente voltado às finalidades às quais a coleta dos dados se destina, respeitando os critérios de compartilhamento e de segurança das informações.

Os dados pessoais devem ser manipulados apenas por pessoas que precisem lidar com eles, reduzindo, assim, os riscos de falhas humanas propiciarem um vazamento ou uso inadequado da informação.

Os dados serão identificados por departamentos e/ou por responsabilidades específicas dentro de cada unidade operacional, a fim de possibilitar conhecer, em cada situação, quem são os operadores dos dados, reduzindo os riscos de um incidente na segurança da informação.

O acesso de cada empregado ou prestador de serviço ao banco de dados do CRCSP é individual e protegido por senha própria e intransferível, garantindo o tratamento dos dados a pessoas autorizadas.

O único tratamento admitido para dados pessoais contidos nos resíduos eletrônicos gerenciados pelo CRCSP é a eliminação.

Parágrafo único. Para garantir que nenhum dos dados que eventualmente estejam armazenados nos dispositivos que o CRCSP gerencia sejam utilizados indevidamente, todos serão destruídos em conformidade com a legislação arquivística vigente que trata sobre a matéria.

O acesso dos empregados e prestadores de serviço do CRCSP aos materiais e às informações contidas no sistema informatizado é restrito de acordo com a autorização determinada na Política de Controle de Acessos do CRCSP.

4. Critérios Estabelecidos

4.1. Coleta dos dados pessoais

As informações referentes às pessoas físicas somente devem ser coletadas na medida da necessidade para a prestação de serviços, para atendimento ao cumprimento das hipóteses cabíveis no art. 7º da LGPD.

O consentimento, quando necessário, é requerido ao solicitar os dados que forem de pessoas físicas, por meio da ciência e do consentimento no campo apropriado em sistema ou por meio de assinatura de termo apropriado dos funcionários, ex-funcionários, conselheiros, delegados representantes, colaboradores e palestrantes.

4.2. Armazenagem dos dados pessoais

Quando armazenados fisicamente, os dados devem ficar em local protegido por tranca, fora do alcance de outras pessoas que não as expressamente autorizadas a acessá-los.

Em caso de necessidade de se armazenar digitalmente dados pessoais fora dos Sistema Informatizados de Bancos de Dados, estes devem ficar em pasta protegida por criptografia ou restrição de acesso por senha pessoal.

Eventuais cópias de dados pessoais somente devem ser feitas, em caso de necessidade, para cumprimento da finalidade proposta ao tratamento dos dados.

4.3. Compartilhamento interno e externo de dados pessoais

Os dados pessoais somente podem ser compartilhados internamente entre as unidades organizacionais cuja função exija acesso e tenha a finalidade ou a obrigação legal para o tratamento dessas informações.

O compartilhamento de dados pessoais com pessoa natural ou jurídica, de direito público ou privado, externas ao CRCSP deve ser restrito ao mínimo necessário para a execução do tratamento em cumprimento de obrigação legal. Mesmo quando o tratamento envolver diretamente a prestação de serviços, o consentimento para este tratamento e compartilhamento deverá ter sido previamente obtido, quando cabível.

É vedado o compartilhamento externo de dados pessoais por qualquer meio, telefônico, digital ou por escrito, não amparado em base legal.

4.4. Período de armazenamento

Os dados pessoais serão armazenados pelo CRCSP durante o período necessário e conforme as finalidades para as quais foram coletados. Esses dados serão mantidos durante o relacionamento com o Titular e/ou pelo tempo obrigatório para cumprirmos com as obrigações legais, contratuais ou regulatórias.

Nos comprometemos a mantê-los armazenados, adotando todas as medidas necessárias e razoáveis para impedir sua alteração, perda e acesso não autorizado, conforme determinação da legislação aplicável e melhores práticas.

5. Encarregado e a prestação das informações

O Encarregado da Proteção de Dados Pessoais será o responsável pela comunicação entre os titulares, o CRCSP e a ANPD, conforme disposto na legislação vigente.

As atividades do Encarregado consistem, conforme o art. 41 da LGPD, em:

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A solicitação quanto à prestação de informações sobre dados pessoais deverá ser encaminhada ao Encarregado da Proteção de Dados Pessoais do CRCSP, para que este promova a resposta ao titular dos dados.

As informações requeridas pelo titular deverão ser sempre evidenciadas de forma transparente, resguardando o sigilo quando aplicável.

Quaisquer questionamentos surgidos acerca da proteção de dados pessoais deverão ser levados ao Encarregado para que este possa orientar de imediato o operador ou buscar junto à ANPD e demais entidades especializadas uma orientação adequada ao questionamento levantado.

O Encarregado da Proteção de Dados Pessoais do CRCSP estará disponível pelo e-mail ouvidoria@crcsp.org.br

Política de Desenvolvimento e Manutenção de Sistemas

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Equipe Técnica

Cláudio Rafael Bifi - **Diretor Executivo**

Domingos Sávio Mota – **Diretor de Tecnologia e Infraestrutura**

Ronaldo César da Silva - **Gerente do Departamento de Tecnologia da Informação**

Cláudio Molina Paes Rosa – **Coordenador de Sistemas do Departamento de Tecnologia da Informação**

Alessandro de Melo Beserra – **Coordenador de Redes e Segurança do Departamento de Tecnologia da Informação**

Política de Desenvolvimento e Manutenção de Sistemas

(Versão 2.0)

REVISÕES		
DATA	AUTOR	VERSÃO
20/09/2017	Claudio Molina Paes Rosa	1.0
12/09/2018	Claudio Molina Paes Rosa	1.0
27/09/2019	Claudio Molina Paes Rosa	1.0
23/12/2020	Claudio Molina Paes Rosa	1.0
21/10/2021	Claudio Molina Paes Rosa	2.0

Sumário

1. Dos motivos

1.1. Ciente da importância em minimizar o impacto de incidentes relacionados a alterações nos sistemas de informação, o Conselho Regional de Contabilidade do Estado de São Paulo - CRC SP passa a implantar a Política de Desenvolvimento e Manutenção de Sistemas.

1.2. A utilização de uma política de desenvolvimento e manutenção de sistemas garante o uso de métodos e procedimentos padronizados para planejamento e execução de todos os passos necessários para o projeto.

1.3. Cabe ao CRC SP, através do departamento de Tecnologia da Informação - TI, o registro e avaliação de todas as solicitações de mudanças de software, calculando os riscos e impactos das alterações solicitadas.

1.4. Toda e qualquer mudança de software só poderá ser executada mediante autorização do departamento de Tecnologia da Informação – TI.

1.5. Tal política deverá ser plenamente atendida por todos os usuários de informática no âmbito do CRC SP que venham solicitar alterações nos sistemas de informação, sendo passível da aplicação das penalidades administrativas correlatas, observadas as normas internas para a ampla defesa.

2. Da solicitação

2.1. A solicitação de uma mudança de software deve partir obrigatoriamente de um usuário com cargo de coordenação ou chefia. Nos casos dos departamentos cuja essa autonomia é dada a um usuário que não seja coordenador ou chefe, o responsável pelo departamento deve comunicar formalmente o departamento de Tecnologia da Informação com antecedência.

2.2. Após a manifestação de interesse inicial, que poderá ser feito por e-mail ou pessoalmente, o departamento de Tecnologia da Informação poderá, se julgar necessário, agendar uma reunião com todos os interessados e/ou envolvidos para levantamento de requisitos e entendimento das regras de negócio.

2.3. Com todas as dúvidas e questionamentos esclarecidos pelos interessados e/ou envolvidos, além do consenso alcançado entre as partes, o departamento de Tecnologia da Informação dará seguimento à documentação necessária para realização da mudança.

3. Da documentação

3.1. As documentações das mudanças de software podem ser simples, resultando apenas na abertura de um chamado no sistema de Help Desk, ou complexas, onde é necessário a criação do documento de desenvolvimento de sistema (Anexo I) antes da abertura do chamado.

3.2. Caberá ao departamento de Tecnologia da Informação, através de sua experiência e conhecimento da mudança solicitada, avaliar os riscos e a complexidade da mudança e definir qual nível de documentação será necessário.

3.3. Em ambos os níveis de documentação, deverá constar claramente todas as solicitações e alterações que serão efetuadas, assim como as regras de negócio específicas da mudança solicitada.

3.4. Mesmo em alterações que exijam o documento de desenvolvimento de sistemas, o chamado no sistema de Help Desk deverá ser aberto após o entendimento completo da solicitação.

3.5. A qualquer momento, o departamento de Tecnologia da Informação – TI poderá, se julgar necessário, anexar à documentação principal, qualquer evidência de solicitação de mudança das regras previamente acordadas e assinadas no documento principal.

3.6. Poderá ser anexada também ao documento principal ou como complemento no chamado no Help Desk, qualquer informação que justifique uma alteração no prazo final do projeto.

3.7. No caso de uma mudança de software que exija o documento de desenvolvimento de sistemas, as mudanças somente terão início após a documentação assinada pelas partes envolvidas.

3.8. Para os casos em que é necessário somente a abertura do chamado, o início do desenvolvimento/alterações se dará assim que houver um analista disponível para executar as mudanças solicitadas.

3.9. Também faz parte da documentação o Termo de Homologação de Sistemas (Anexo II), que será explicado no item 5 – Da homologação.

4. Dos prazos

4.1. O prazo para a conclusão de cada etapa do projeto estará especificado na documentação de sistema, bem como o prazo final para que todo o trabalho seja entregue.

4.2. Para a estimativa do prazo de conclusão, serão considerados o levantamento de requisitos além da complexidade de cada etapa do projeto.

4.3. Em algumas situações poderá ocorrer alterações no prazo estipulado na documentação de sistema. Segue abaixo:

a) Interrupções do trabalho do analista alocado por mudança de prioridade;

b) Alterações nas regras e/ou recursos não descriminados no escopo do projeto;

c) Problemas ou impactos que são detectáveis apenas durante o desenvolvimento pelo analista alocado;

4.4. A contagem do prazo sempre será em dias úteis e terá início a partir do primeiro dia a contar da assinatura da documentação do sistema.

5. Da homologação

5.1. Ao término do trabalho, o analista alocado para efetuar as mudanças no sistema, notificará o usuário responsável pela solicitação e pedirá que faça testes para homologar as alterações efetuadas.

5.2. A critério do analista, os testes poderão ser efetuados na máquina do usuário ou no próprio departamento de TI junto com o analista.

5.3. Os passos 5.1 e 5.2 se repetirão enquanto houver problemas ou enquanto as mudanças não atenderem por completo a solicitação, conforme especificado na documentação principal.

5.4. Após a entrega completa do projeto e exclusivamente nos casos em que foi elaborado o documento de desenvolvimento de sistemas, será pedido ao usuário responsável pela solicitação, que preencha o Termo de Homologação de Sistemas (Anexo II), onde poderá avaliar o atendimento e registrar pontos que julgar importante.

5.5. Com o Termo de Homologação assinado ou nos casos em que não exista o documento de desenvolvimento de sistema, após a entrega completa do projeto, o analista poderá fechar o chamado aberto e assim concluir a solicitação.

6. ANEXO I

MODELO DE DOCUMENTAÇÃO PARA DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

SÃO PAULO – <ANO>

SUMÁRIO

1. APRESENTAÇÃO

Descrever como funciona atualmente o procedimento do departamento, e como ficará após a implementação do Sistema.

2. DEFINIÇÃO DE ESCOPO

<Título do Sistema>

[X] **Novo Projeto** [ ] **Alteração** [ ] **Melhoria**

Descrever detalhadamente, o que exatamente será objeto de implementação/alteração, deixar claro coisas que não serão alteradas.

3. ESPECIFICAÇÃO DE REQUISITOS

Requisito	**Responsável**
Requisito 1	*Depto XX*
Requisito 2	*Depto XX*
Requisito 3	*Depto XX*
Requisito 4	*Depto XX*

4. PROTÓTIPOS DE INTERFACE DO USUÁRIO

Incluir os protótipos de telas a serem desenvolvidas/alteradas, quando for o caso, se não houver necessidade, esse tópico poderá ser eliminado

5. PRAZOS E ACEITE

ETAPAS / TELAS	PRAZO EM DIAS	RESPONSÁVEL
Etapa 1	*5*	*Analista 1*
Etapa 2	*5*	*Analista 1*
Etapa 3	*5*	*Analista 2*
Etapa 4	*5*	*Analista 2*
Etapa 5	*5*	*Analista 3*
Etapa 6	*5*	*Analista 3*
TOTAL	30 DIAS ÚTEIS	

São Paulo, <data>

_____
<Gestor do Depto. TI>
<Cargo do Gestor do Depto. TI>

_____
<Nome do Gestor do Departamento Requisitante>
<Cargo do Gestor do Departamento Requisitante >

6. ALTERAÇÕES SOLICITADAS

Incluir na tabela abaixo o histórico das alterações que foram solicitadas, informando o número do chamado, data e descrição na tabela.

Nº Chamado	Data	Descrição

7. ANEXO II

TERMO DE HOMOLOGAÇÃO DE DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

DEPTO. TECNOLOGIA DA INFORMAÇÃO

DATA / /

TERMO DE HOMOLOGAÇÃO DE SISTEMAS

MÓDULO/SISTEMA	LOCAL	Nº DOCUMENTO

PARTICIPANTES

NOME	DPTO.	RÚBRICA

PONTOS IDENTIFICADOS

AJUSTES E/OU ALTERAÇÕES, NÃO CONSTANTES DA ESPECIFICAÇÃO, A SEREM IMPLEMENTADOS EM MOMENTO POSTERIOR

A HOMOLOGAÇÃO ATENDE DE FORMA SATISFATÓRIA TODAS AS EXIGÊNCIAS DO CICLO DE TESTES DE SISTEMAS:

FUNCIONALIDADE		USABILIDADE		CONFIABILIDADE	
EFICIÊNCIA		MANUTENIBILIDADE		PORTABILIDADE	

ATESTO QUE OS PRODUTOS GERADOS NA HOMOLOGAÇÃO FORAM AVALIADOS E APROVADOS POR ESTAREM EM CONFORMIDADE COM A ESPECIFICAÇÃO

DE ACORDO:

GESTOR USUÁRIO	RESPONSÁVEL TI
NOME:	**NOME:**
DEPARTAMENTO:	**CARGO:**

Plano de Continuidade de Negócios de TI

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Equipe Técnica

Cláudio Rafael Bifi - **Diretor Executivo**

Domingos Sávio Mota – **Diretor de Tecnologia e Infraestrutura**

Ronaldo César da Silva - **Gerente do Departamento de Tecnologia da Informação**

Cláudio Molina Paes Rosa – **Coordenador de Sistemas do Departamento de Tecnologia da Informação**

Alessandro de Melo Beserra – **Coordenador de Redes e Segurança do Departamento de Tecnologia da Informação**

Plano de Continuidade de Negócios de TI

(Versão 3.0)

REVISÕES		
DATA	AUTOR	VERSÃO
19/08/2016	Claudio Molina Paes Rosa	1.0
01/03/2018	Ronaldo Cesar da Silva	2.0
19/10/2021	Claudio Molina Paes Rosa	3.0

Sumário

1. Introdução

O Plano de Continuidade de Negócios de Tecnologia da Informação (PCNTI) contém medidas preventivas, procedimentos de recuperação em eventuais interrupções de negócios, além de assegurar a identificação, avaliação, monitoramento e controle dos recursos que dão suporte à realização das operações (equipamentos, sistemas de informações, pessoal, instalações e informações).

O PCNTI abrange as estratégias necessárias à continuidade dos serviços de TI essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TI do CRCSP e serviços essenciais, de acordo com o Decreto-Lei n.º 9.295/46 e alterações, para o registro, a fiscalização do exercício da profissão contábil, a normatização e a educação profissional continuada.

O PCNTI é executado tanto no âmbito do TI quanto isoladamente, ou como parte de um Plano de Continuidade de Negócios (PCN) do CRCSP.

Os sistemas gerenciados pelo CRCSP, assim como os recursos que estão dentro da infraestrutura de tecnologia da informação, são serviços essenciais à ativa do CRCSP.

A infraestrutura de tecnologia da informação se encontra na própria sede do CRCSP, se baseando na estrutura com todos os serviços básicos de infraestrutura, como instalações elétricas adequadas, com gerador e no-breaks, ar-condicionado, links de comunicação e equipamentos de conectividade.

Um dos pilares do plano de continuidade de do CRC SP é o procedimento do TI 002, que trata do Backup Geral da Rede, sobre os procedimentos de backup e restore, e os testes que são executados.

1. Objetivos

O PCNTI foi elaborado para atingir os seguintes objetivos:

a) Assegurar integridade, segurança, qualidade, confidencialidade e acessibilidade dos dados e informações;

b) Obter capacidade de gerenciar uma interrupção no negócio de forma a evitar impactos para o registro, a fiscalização do exercício da profissão contábil, a normalização e a educação profissional continuada, a fim de proteger a reputação da organização;

c) Manter os sistemas e infraestruturas tecnológicas consideradas essenciais disponíveis;

d) Melhorar proativamente a resiliência da organização em momentos necessários, mitigar os riscos de interrupções e diminuindo o tempo de resposta a possíveis incidentes; e

e) Assegurar através de método sistemático o retorno de operacionalização, em um tempo aceitável dos serviços críticos, após um incidente.

2. Sistemas Essenciais

Os sistemas na tabela abaixo por ordem de prioridade são considerados essenciais para o acionamento e execução do PCNTI:

Sistema	Criticidade	RPO[1]	RTO[2]	Impacto			
				Financeiro	Legal	Imagem	Operacional
Serviços Online	Alta	24 horas	6 horas	Alto	Alto	Alto	Alto
Sistema de Gestão Protheus (TOTVS)	Alta	24 horas	6 horas	Médio	Alto	Alto	Alto
Portal Institucional (crcsp.org.br)	Alta	24 horas	6 horas	Alto	Médio	Alto	Médio
SPI (desktop)	Alta	24 horas	6 horas	Alto	Médio	Alto	Médio
CRC SP Mobile (App)	Média	48 horas	16 horas	Médio	Baixo	Alto	Médio
CRC SP Flow (Intranet)	Média	48 horas	16 horas	Baixo	Baixo	Médio	Médio

[1] RPO: ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura

[2] RTO: período dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.

3. Infraestruturas Tecnológicas

Além dos sistemas descritos anteriormente, existem os ativos referentes às infraestruturas físicas, nos quais também são considerados serviços essenciais.

Ativo	Criticidade	Prioridade	Impacto			
			Financeiro	Legal	Imagem	Operacional
Rede de Dados Interna (LAN)	Alta	Alta	Alto	Baixo	Alto	Alto
Link de Dados (WAN)	Alta	Alta	Alto	Baixo	Alto	Alto
Servidor Telefonia	Alta	Alta	Alto	Baixo	Alto	Alto
Energia Elétrica	Alta	Alta	Alto	Médio	Alto	Alto

4. Desastres e Catástrofes Naturais ou Não

Em casos de incidentes, tais como incêndio, não acesso ou outros desastres naturais ou acidentais, após as ações iniciais para contenção dos incidentes, o Comitê de Tecnologia da Informação (CTI) deverá se reunir para identificar os danos causados e assim definir se o PCNTI será acionado.

Serão emitidos relatórios aos Gestores para conhecimento e adoção de medidas julgadas necessárias.

5. Invocação do Plano

O Plano de Continuidade será acionado quando ocorrer algum dos cenários de desastres, insurgência ou ocorrência de um risco desconhecido, e ainda se houver uma vulnerabilidade que tenha grande possibilidade de ser explorada. Poderá invocar o PCTI em casos de testes, ou por determinação do Comitê de TI juntamente com a alta administração do CRC SP.

Os planos de continuidade serão encaminhados para aprovação da Alta Gestão e pelo responsável da Infraestrutura de TI, inseridos os incidentes de interrupção. Interação com áreas provedoras de recursos para operacionalização (TI, Comunicação Social, entre outras).

Os integrantes das equipes, após acionados, iniciarão a avaliação e investigação do ocorrido, podendo acionar outras equipes, caso necessário.

6. Tabela de Responsáveis

Abaixo, segue os contatos dos responsáveis pelas ações a serem tomadas em caso de ocorrência de desastres:

Cargo/ Empresa	Nome	Telefone / Celular

7. Principais Riscos

O PCNTI foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam riscos à continuidade dos serviços essenciais.

O quadro a seguir define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
01- Interrupção de energia elétrica	- Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 24 (vinte e quatro) horas; - Causada por fator interno que comprometa a rede elétrica do prédio com curtos-circuitos, incêndio e infiltrações; - Impossibilidade de acionar o Grupo gerador no momento de uma queda de energia.
02 - Falha na Climatização do CPD	- Superaquecimento dos ativos devido à falha no dimensionamento de carga; - Falha na unidade de climatização e não emissão de alertas de monitoração.
03 - Indisponibilidade de Backup	- Cópia de segurança dos dados não disponível ou sem integridade.
04 - Indisponibilidade de rede/circuitos	- Rompimento de fibra ótica decorrente de execução de obras públicas, desastres ou acidentes; - Mal funcionamento de *switch* gerenciador de segmento de rede; - Interrupção dos serviços de conectividade com as operadoras de telecomunicação por mais de 12 (doze) horas.
05 - Falha humana	- Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível.
06 - Ataques internos	- Ataque aos ativos do *Data Center e à rede CRCSP*.
07 - Incêndio	- Falhas nos equipamentos ou por ação humana.
08 - Falha de hardware	- Falha que necessite reposição de hardware crítico ou reparo, e cujo reparo ou aquisição dependa de processo licitatório.
09 - Ataque cibernético	- Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais, assim como a indisponibilização dos dados por meio de deleção ou mesmo sequestro virtual.

8. Planos de Contingência para Incidentes

Na sequência são apresentados os planos de ação, divididos por ativo da empresa considerados essenciais com risco de falhas de impacto:

Ativo: Serviços Online

AMEAÇAS	VULNERABILIDADE	RISCOS
Acesso indisponível ou funcionamento de forma inesperada (bug).	Erros de programação ou problemas físicos	Interrupção das atividades finalísticas

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Solicitar à equipe de desenvolvimento uma análise e correção do problema.	Coordenador de Sistemas	6 horas	Implantar ação imediatamente
Solicitar à equipe de rede/suporte uma análise quanto à infraestrutura	Coordenador de Sistemas	6 horas	Implantar ação imediatamente

Ativo: Sistema de Gestão Protheus (TOTVS)

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha do Sistema.	Impacto nos Processo que utilizam o Sistema.	Atualização de versão com falha.

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer o sistema de forma funcional.	Assistente de Suporte Técnico.	6 horas	Implantar ação imediatamente.
Reestabelecer a funcionalidade física do servidor (componentes eletrônicos)	Administrador de Rede.	6 horas	Implantar ação imediatamente.
Reestabelecer a funcionalidade do banco de dados do servidor (base de dados).	Coordenador TI.	6 horas	Implantar ação imediatamente.
Viabilizar provisionamento para substituição do equipamento em caso de falha e/ou criação de ambiente redundante.	Diretor TI, Gerente TI, Coordenador TI e Administrador de rede.	6 horas	Implantar ação imediatamente.

Ativo: Portal Institucional (crcsp.org.br)

AMEAÇAS	VULNERABILIDADE	RISCOS
Portal Institucional indisponível	Falhas de DNS ou interrupção do serviço de hospedagem	Perda de acesso dos profissionais e da sociedade ao portal

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Checagem da infraestrutura de rede	Administrador de Rede	6 horas	Implantar ação imediatamente.
Abrir chamado na empresa de hospedagem	Administrador de Rede.	6 horas	Implantar ação imediatamente.

Ativo: SPI (Desktop)

AMEAÇAS	VULNERABILIDADE	RISCOS
Acesso indisponível ou funcionamento de forma inesperada (bug).	Erros de programação ou problemas físicos	Interrupção das atividades finalísticas

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Solicitar à equipe de desenvolvimento uma análise e correção do problema.	Coordenador de Sistemas	6 horas	Implantar ação imediatamente
Solicitar à equipe de rede/suporte uma análise quanto à infraestrutura	Coordenador de Sistemas	6 horas	Implantar ação imediatamente

Ativo: CRC SP Mobile (App)

AMEAÇAS	VULNERABILIDADE	RISCOS
Acesso indisponível ou funcionamento de forma inesperada (bug).	Erros de programação ou problemas físicos	Interrupção dos recursos do aplicativo para os profissionais

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Solicitar à equipe de desenvolvimento uma análise e correção do problema.	Coordenador de Sistemas	16 horas	Implantar ação em médio prazo
Solicitar à equipe de rede/suporte uma análise quanto à infraestrutura	Coordenador de Sistemas	16 horas	Implantar ação em médio prazo

Ativo: CRC SP Flow (Intranet)

AMEAÇAS	VULNERABILIDADE	RISCOS
Interrupção do Serviço de Intranet, falha no servidor responsável por suportar o serviço intranet.	Fornecimento de acesso ao serviço intranet interrompido.	Perda de acesso os serviços disponibilizados na intranet

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Efetuar o procedimento corretivo utilizando-se de backup para restauração mais relevante do ambiente intranet	Coordenador de TI e Assistente de Suporte Técnico	16 horas	Implantar ação em médio prazo.
Contatar empresa TOTVS que dá suporte ao serviço.	Coordenador de TI e Assistente de Suporte Técnico	16 horas	Implantar ação em médio prazo.

Ativo: Rede de Dados Interna (LAN)

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha no equipamento (switch).	Fornecimento de acesso à rede de forma interrompida, por inexistência de redundância.	Parada da rede Corporativa –LAN.

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados interna (LAN).	Administrador de Rede.	Interrupção não tolerável.	Implantar ação imediatamente.
Viabilizar a disponibilização da rede em modo redundante.	Gerente de TI, Administrador de Rede.		Implantar ação em médio prazo.

Ativo: Link de Dados (WAN) - Internet

AMEAÇAS	VULNERABILIDADE	RISCOS
Interrupção do Serviço de fornecimento de acesso internet (WAN) pelo prestador do serviço e falha no equipamento.	Fornecimento de acesso à internet de forma interrompida.	Perda de acesso à internet com indisponibilidade dos serviços de e-mail, WEB e com possibilidade de perdas de transações eletrônicas.

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados WAN.	Administrador de Rede.	Interrupção não tolerável	Implantar ação imediatamente.
Viabilizar o fornecimento de acesso em modo redundante para disponibilizar o acesso a internet e seus serviços de forma ininterrupta.	Gerente de TI e Administrador de Rede.		

Ativo: Servidor Telefonia

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha nos equipamentos.	Fornecimento de serviço de voz interrompido por falha adversa, sem aviso prévio e por inexistência de redundância.	Perder a comunicação via telefone com as entidades externas à empresa (CFC, outros CRC´S, delegacias, conselheiros, profissionais da contabilidade e público em geral).

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Utilizar de forma emergencial os telefones celulares corporativos	Gerente de TI e Administrador de Rede.	Interrupção não tolerável.	Implantar ação imediatamente.
Contatar empresa Betta que dá suporte ao serviço.	Administrador da Rede.	Interrupção não tolerável.	Implantar ação imediatamente.

Ativo: Energia Elétrica

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha na prestação do serviço	Fornecimento de energia interrompida por falta de redundância.	Interromper a operação da empresa

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Executar medidas para preservação dos equipamentos de TI	Gerente de TI e Administrador de Rede.	4 horas	Implantar ação imediatamente.
Contatar o chefe da manutenção sobre prazos de restabelecimento da energia.	Chefe da Manutenção	4 horas	Implantar ação imediatamente.

Política de Impressão

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Equipe Técnica

Cláudio Rafael Bifi - **Diretor Executivo**

Domingos Sávio Mota – **Diretor de Tecnologia e Infraestrutura**

Ronaldo César da Silva - **Gerente do Departamento de Tecnologia da Informação**

Cláudio Molina Paes Rosa – **Coordenador de Sistemas do Departamento de Tecnologia da Informação**

Alessandro de Melo Beserra – **Coordenador de Redes e Segurança do Departamento de Tecnologia da Informação**

Política de Impressão

(Versão 1.0)

REVISÕES		
DATA	AUTOR	VERSÃO

Sumário

1. Dos motivos

1.1. Promover o uso racional do recurso, reduzindo custos e impacto ambiental decorrente da produção e descarte dos insumos;

1.2. Regular o uso do serviço de acordo com a legislação vigente e aplicável;

1.3. Reunir e documentar práticas adotadas na instituição;

1.4. Esclarecer aos usuários direitos e responsabilidades no uso do serviço;

2. Definições

2.1. Impressora: dispositivo usado para impressão monocromática ou colorida de documentos, podendo operar com papéis de tamanhos variados;

2.2. Insumos: materiais necessários a operação da impressora, que incluem tanto material básico (papel, toner) quanto peças de uso interno que têm vida útil controlada (fusor, etc.);

2.3. Centro de Custo: Denominam-se centros de custos os diversos departamentos do CRCSP;

2.4. Vínculo institucional: relação formal e ativa de uma pessoa com o CRCSP: funcionários, prestadores de serviços e conselheiros;

2.5. Colaboradores: Pessoas que estejam realizando atividades que coadunam com os objetivos e fins da instituição e que justifiquem a necessidade de uso deste serviço em função da natureza de seu vínculo institucional, devendo sua identidade ser validada por funcionário técnico administrativo do CRCSP;

3. Finalidade e Uso

3.1. O serviço de Impressão destina-se exclusivamente a atividades do CRCSP;

3.2. A sustentabilidade ambiental é elemento chave na utilização do serviço – a impressão de documentos deve ser evitada sempre que possível;

3.3. Deve-se sempre usar impressão em face dupla;

3.4. Deve-se, se possível, imprimir em modo econômico;

3.5. Evitar a impressão de várias cópias de um mesmo documento, exceto quando houver real necessidade;

3.6. Deve-se buscar a tramitação de processos administrativos sempre na forma eletrônica, fazendo uso da impressão apenas nos casos em que se requer assinatura ou carimbos impressos;

3.7. As impressoras são alocadas nos centros de custo conforme demandas apresentadas;

3.8. É de responsabilidade dos centros de custo a alocação racional deste recurso, reduzindo custos pelo compartilhamento de equipamentos;

3.9. Toda impressão realizada através do serviço deve ser associada a um único usuário;

3.10. É de responsabilidade do colaborador manter o sigilo de sua senha(token) de acesso à impressora;

3.11. Informações sobre o número de páginas e título dos documentos, assim como data e hora da impressão, assim como o usuário responsável, são registradas e mantidas por tempo indeterminado;

3.12. Utilizar a impressora colorida somente para documentos que necessitem de impressão colorida, pois os custos são maiores em relação a impressora mono;

3.13. Os centros de custo são responsáveis por indicar um responsável pelo acompanhamento do serviço em sua unidade;

3.14. O responsável pelo centro de custo poderá implementar uma política de quotas de impressão.

3.15. Os custos associados ao serviço serão repassados aos respectivos centros de custos.

4. Infraestrutura do serviço de impressão

4.1. O serviço de impressão é provido para uso departamental – ele deve ser composto por uma ilha de impressão em cada departamento, visando racionalizar recursos de energia elétrica, espaço físico, consumo de papel, gestão de suprimentos, administração e gerência;

4.2. As unidades contempladas recebem equipamentos que são contratados na forma de serviço e incluem manutenção de defeitos, fornecimento de tôner e outros suprimentos, descarte e reciclagem de partes e peças substituídas. Somente o papel deve ser fornecido pela unidade usuária do serviço;

4.3. A manutenção das impressoras opera de modo proativo, substituindo insumos antes que gerem parada do serviço (por exemplo, troca de toner);

4.4. São fornecidos diferentes modelos de impressora com custos e capacidades diferenciados;

4.5. Cada impressora tem um custo fixo por página, conforme seu modelo;

4.6. Poderá existir uma franquia de impressão, que estabelece o quantitativo máximo de impressões para viabilizar o planejamento financeiro dos serviços.

4.7. O serviço de impressão implementará um mecanismo de segurança, que habilita a impressão somente quando o usuário estiver perto da impressora.

4.8. Poderão ser implementados mecanismos para redução de impressão como limite de páginas de um documento, redirecionamento de documentos grandes para impressoras com custo menor, limite de cópias de documentos, tempo mínimo entre impressões, tempo de descarte e obrigatoriedade da autorização presencial para início da impressão.