
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.