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.