

Protocolo — Criação de Contas de Usuário

Setor responsável: T.I.

Público-alvo: Novos servidores, docentes e colaboradores do COPPEAD

Pré-requisito obrigatório: Solicitação formal do RH

1. Objetivo

Estabelecer o fluxo padrão para criação de contas de acesso (rede, e-mail institucional e sistemas internos) de novos usuários do COPPEAD, assegurando que toda criação de conta seja formalmente autorizada e rastreável, em conformidade com boas práticas de gestão de identidade e controle de acesso.

2. Regra fundamental

O setor de T.I. NÃO cria nenhuma conta de usuário por solicitação verbal, de terceiros ou do próprio interessado. A criação de conta só é realizada mediante e-mail oficial do Recursos Humanos (RH) do COPPEAD, solicitando expressamente a abertura da conta.

3. Fluxo do processo

1. O RH formaliza a admissão/vínculo do novo usuário e envia e-mail ao setor de T.I. solicitando a criação da conta, informando: nome completo, CPF, cargo/função, setor de lotação, data de início das atividades e e-mail pessoal para contato.
2. O setor de T.I. cria a conta de rede/domínio, o e-mail institucional e os acessos aos sistemas necessários à função, conforme perfil de acesso padrão definido para o cargo.
3. É gerada uma senha provisória, configurada para troca obrigatória no primeiro acesso.
4. O setor de T.I. confirma ao RH, por e-mail, a conclusão da criação da conta.
5. As credenciais são entregues ao RH, que fica responsável por entregá-las diretamente ao usuário.

4. Situações não cobertas por este protocolo

- Solicitações de criação de conta feitas diretamente pelo interessado, por chefias ou por terceiros, sem e-mail do RH — devem ser recusadas e redirecionadas ao RH.
- Alterações de perfil de acesso por mudança de função: também dependem de comunicação formal do RH ou da chefia imediata, com anuência do RH.
- Contas para prestadores de serviço, estagiários ou visitantes temporários: seguem o mesmo princípio — exigem solicitação formal do setor responsável pela contratação (RH ou coordenação), com prazo de validade definido.

5. Desligamento e bloqueio de conta

De forma simétrica, o bloqueio ou exclusão de contas por desligamento também deve ser solicitado formalmente pelo RH, informando a data de término do vínculo, para que o acesso seja suspenso imediatamente na data correta.

6. Boas práticas de segurança aplicadas

- Padronização do nome de usuário e do e-mail institucional.
- Aplicação do princípio do menor privilégio: acesso liberado apenas ao necessário para a função.

- Registro de todas as solicitações e ações em log/controle interno do setor de T.I., para fins de auditoria.
- Revisão periódica das contas ativas em conjunto com o RH, para identificar contas de usuários já desligados.