# 1. ÍNDICE

[1. ÍNDICE 2](#_Toc163233241)

[2. Objetivo 3](#_Toc163233242)

[3. Definições e Abreviações 3](#_Toc163233243)

[4. Responsabilidades 4](#_Toc163233244)

[5. Procedimento 4](#_Toc163233245)

[5.1. Procedimento de Controle de acesso 4](#_Toc163233246)

[5.2 Procedimentos de controle de acesso de novo usuário 5](#_Toc163233247)

[5.3 Procedimentos para alteração de perfil, bloqueio de acesso e remoção de usuário. 6](#_Toc163233248)

[5.4 Criação/alteração de Lista de usuário no sistema. 7](#_Toc163233249)

[5.5 Gerenciamento de senhas 7](#_Toc163233250)

[5.6 Perfis de Acesso 8](#_Toc163233251)

[5.7 Gerenciamento de Segurança 12](#_Toc163233252)

[5.8 Acesso ao gerenciamento de data e hora 13](#_Toc163233253)

[6. Referências 13](#_Toc163233254)

[7. Histórico 13](#_Toc163233255)

[8. VALIDAÇÃO 14](#_Toc163233256)

[9. Anexos 14](#_Toc163233257)

# 2. Objetivo

O presente POP tem como finalidade estabelecer uma abordagem estruturada e segura para a criação e administração de contas de usuários em sistemas, visando assegurar a integridade, confidencialidade e disponibilidade dos recursos e informações corporativas.

# 3. Definições e Abreviações

Sistema informatizado: Sistema informatizado que controla o desempenho de um ou mais processos de negócios automatizados. Inclui *hardware*, *software*, periféricos, redes, pessoal e documentação (manuais e procedimentos operacionais padrão).

Processamento de dados: Sequência de operações executadas nos dados a fim de extrair, apresentar ou obter informações em um formato definido.

Registro Híbrido: Registro híbrido é uma combinação de registros eletrônicos originais e registros em papel.

Registro original: registros de dados como o arquivo ou o formato no qual ele foi originalmente gerado, preservando a integridade (exatidão, integralidade, conteúdo e intenção) do registro. Ex: Observação manual de registro original em papel ou arquivos de dados brutos eletrônicos de um sistema informatizado. Esses dados devem permitir a reconstrução completa das atividades resultando na geração de dados.

Dados brutos: Registros originais e documentação, mantido no formato em que eles foram originalmente gerados (ou seja, em papel ou eletrônicos), ou como uma 'cópia'. Dados brutos devem ser simultaneamente e precisamente gravados por meios permanentes.

Dados Regulamentados: utilizados para fins GxP relevantes e exigidos pelos regulamentos GxP.

Perfil de usuário: Um perfil de usuário é um registro de dados específicos do usuário que define o ambiente de trabalho do usuário em relação a um determinado sistema informatizado. O perfil pode incluir configurações de vídeo, configurações de aplicativos e conexões de rede. Os Arquivos, aplicativos, diretórios que têm acesso e os direitos que eles possuem em um sistema é determinado pelo dono do sistema e administrador.

Controle de acesso: Controle de acesso é a restrição seletiva de acesso a um lugar, um sistema informatizado ou outro recurso. Controle de acesso físico pode ser alcançado por um ser humano, através de meios mecânicos como fechaduras e chaves, ou através de meios tecnológicos, tais como sistemas de controle de acesso (crachá, biométrico, etc.).

BIOS: Conhecido como o BIOS do sistema, é um Acrônimo para *Basic Input/Output System*. É um tipo de *firmware* usado para executar a inicialização de *hardware* durante o processo de ligar um computador para o funcionamento de sistemas e programas.

Administrador: uma pessoa que é responsável pelo acesso, manutenção, configuração e operação confiável dos sistemas informatizados ou computadores multiusuários.

Supervisor: Pessoa responsável por gerenciar e fazer modificações controladas em receitas e relatórios.

Usuário: Pessoa responsável pelo funcionamento do equipamento, seguindo o procedimento padrão.

TI: Tecnologia da Informação*.*

GxP: *Good X Practices* (Boas práticas, sendo x = Distribuição, Laboratório e Fabricação).

POP: Procedimento Operacional Padrão

KeyUser Local: Especialista local responsável pelo sistema.

# 4. Responsabilidades

A execução deste processo é em colaboração com a equipe de segurança da informação de projetos.

# 5. Procedimento

## 5.1. Procedimento de Controle de acesso

5.1.1. Os procedimentos de controle de acesso para sistemas gerenciados localmente incluem:

5.1.2. IDs individuais de usuários;

5.1.3. O dono do sistema e o administrador do sistema devem aprovar o pedido para conceder acesso ao sistema informatizado somente após garantir que o usuário recebeu treinamento no sistema computadorizado.

5.1.4. Descrição dos direitos de acesso dos usuários;

5.1.5. Declaração formal dos usuários (assinatura) com o compromisso na utilização da assinatura eletrônica e da confidencialidade da senha de acesso na utilização do sistema computadorizado;

5.1.6. Garantir que os administradores não forneçam acesso até que os procedimentos de autorização de acesso tenham sido concluídos;

5.1.7. Remover ou bloquear os direitos de acesso dos usuários quando eles não são mais necessários.

## 5.2 Procedimentos de controle de acesso de novo usuário

5.2.1. O dono do sistema deve elaborar e preencher um Formulário de Gerenciamento de Acessos aos Sistemas GxP.

5.2.2.1. Selecionar o tipo de conta: concessão de acesso, mudança de perfil, bloqueio de acesso ou remoção de acesso;

5.2.2.2. Nome do usuário: descrever o nome do usuário para o qual está requisitando acesso;

5.2.2.3. ID do usuário: nome da conta de acesso;

5.2.2.4. Grupo de trabalho;

5.2.2.5. Departamento: descrever o departamento do usuário;

5.2.2.6. Dono do Processo: nome do dono do processo;

5.2.2.7. Aprovação do Usuário: declaração de acordo de compromisso do usuário na utilização da assinatura eletrônica e da confidencialidade da senha de acesso;

5.2.2.8. Registro dos acessos que serão concedidos pelo administrador;

5.2.2.9. Sistema (TAG) – descrição do sistema que deverá ter acesso;

5.2.2.10. POP/TI: Informação do POP/TI cujo treinamento é obrigatório para ter acesso ao sistema.

Nota: Caso seja necessária a realização de outros treinamentos, complementar na linha logo abaixo.

5.2.2.11. Data do treinamento – Preencher a data do treinamento realizado;

5.2.2.12. Treinamento realizado por: nome do instrutor responsável pelo treinamento.

5.2.2.13. Perfil de acesso – descrição do perfil necessário (Analista/operador, supervisor, manutenção, administrador, etc).

5.2.2.14. O administrador do sistema deve registrar sua aprovação mediante recebimento do Formulário de Gerenciamento de Acessos aos Sistemas GxP com todas as informações acima preenchidas;

5.2.2.15. O administrador registra a data da criação do acesso e devolve o formulário para o dono do sistema;

5.2.2.16. O dono do sistema assina e arquiva o formulário na área de trabalho.

Nota: O gestor somente deve assinar o Formulário de Gerenciamento de Acessos aos Sistemas GxP após o administrador concluir os acessos nos sistemas.

5.2.2.17. O dono do sistema assina e arquiva o formulário na área de trabalho.

## 5.3 Procedimentos para alteração de perfil, bloqueio de acesso e remoção de usuário.

****6.3.1. As contas de usuários que não estão mais autorizadas a fazer login, entrada, alterar ou excluir dados no sistema (por exemplo, devido a mudança de função ou rescisão de contrato de um funcionário) devem ser desativadas em tempo hábil com base na criticidade dos dados do sistema, conforme tabela 1.

Tabela 1

|  |  |
| --- | --- |
| **Criticidade de dados do sistema** | **Prazo para atualizar/desativar a conta do usuário** |
| Alta | Dentro de 1 semana após a mudança de função ou rescisão de contrato. |
| Média | Dentro de 2 semanas após a mudança de posição ou rescisão de contrato. |
| Baixa | Dentro de um mês após a mudança de posição ou rescisão de contrato. |

5.3.3. Repetir o passo 5.2.1, selecionando a opção desejada (remoção, alteração ou bloqueio) e preenchendo as informações dos itens seguintes.

5.3.4. Este novo formulário deve ser anexado ao formulário anterior.

Nota: Caso o usuário seja desligado, a assinatura do usuário não é necessária. Neste caso, o dono do sistema descreve “DESLIGAMENTO”.

## 5.4 Criação/alteração de Lista de usuário no sistema.

5.4.1. O administrador do sistema deve criar, manter atualizada a lista dos usuários aos sistemas.

5.4.2. A Lista tem que estar disponível para consulta.

Nota: É permitido utilizar uma listagem de usuários para contemplar os acessos à equipamentos iguais.

## 5.5 Gerenciamento de senhas

****6.5.1. Para sistemas conectados à rede de TI ou sistemas standalone o gerenciamento de senhas deve ser de acordo com a tabela 2

Tabela 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Controle de acesso para sistemas electrônicos Standalone** | **Criticidade dos dados** | | | |
| **Alta** | **Média** | | **Baixa** |
| Método de acesso | Usuário individual (ID do usuário e senha) | | | |
| Comprimento da senha | 8 caracteres | | | |
| Expiração de senha | A cada 90 dias | A cada 180 dias | Anualmente | |
| Bloqueio da conta após repetidas entradas de senha incorretas | 5 entradas de senha incorretas | 10 entradas de senha incorretas | 15 entradas de senha incorretas | |
| Histórico de senhas (reutilização de senha usada anteriormente) | 10 ciclos | 5 ciclos | 2 ciclos | |
| Logout de inatividade | 5 min. | 15 min. | 30 min. | |

5.5.2.1. Ao comprar novos sistemas informatizados, as diretrizes da tabela 2 devem fazer parte das especificações técnicas.

5.5.2.2. Caso o *software* não seja totalmente compatível com esses requisitos, deve ser realizada uma análise de risco para mitigar o requerimento que não é suportado pelo sistema. A mitigação pode resultar na utilização de funcionalidades do sistema operacional ou através das seguintes informações descritas nos procedimentos escritos dos equipamentos/sistemas:

5.5.3. Histórico de senhas: obrigatoriedade em não reutilizar senhas;



5.5.4. Logout Manual: o usuário deve sair do sistema ao se ausentar da sala ou finalizar a análise.

## 5.6 Perfis de Acesso

5.6.1. Todas as funções de acesso são definidas e documentadas. O administrador do sistema deve garantir que o acesso do administrador do sistema seja restrito a pessoas autorizadas e não seja usado para operações de rotina. Os administradores de sistemas ou supervisores de laboratório devem manter uma lista atualizada com as contas e os direitos de acesso dos usuários no sistema.

5.6.2. Os direitos de acesso (ou trilhas de auditorias) do usuário devem impedir alterações de dados não autorizados. Todas as modificações devem ser registradas pela trilha de auditoria e todos os dados (originais e modificados) devem estar disponíveis.

5.6.3. Deve-se usar todos os controles de acesso para garantir que as pessoas tenham acesso apenas as funcionalidades adequadas à função de trabalho e que as ações sejam atribuídas a um indivíduo específico, conforme descrito no item 5.1.1.

5.6.4. Deve ser capaz de demonstrar os níveis de acesso concedidos a funcionários individuais e garantir que informações históricas sobre o nível de acesso do usuário estejam disponíveis por onze anos para cumprir os requisitos das agências.

5.6.5. Os controles devem ser aplicados no sistema operacional e aplicativos, sem esquecer de proteger e controlar a BIOS (por senha, por exemplo).

5.6.6. Os *logs* compartilhados ou acesso genérico aos usuários não devem ser permitidos.

5.6.7. Onde o *design* do sistema computadorizado suporta acesso individual ao usuário, esta função deve ser usada. Isso pode exigir a compra de licenças adicionais.

5.6.8. É reconhecido que alguns sistemas informatizados suportam apenas um *login* de usuário único ou um número limitado de logins de usuários. Quando nenhum sistema informatizado alternativo adequado está disponível, um controle equivalente pode ser fornecido por *software* de terceiros ou um método baseado em *logbook* para fornecer a rastreabilidade (descrito em procedimentos e com controle de versão). A adequação de sistemas alternativos deve ser justificada e documentada (relatório de qualificação, POP e análise de risco para sistemas informatizados). É provável que seja necessária uma verificação maior na análise dos dados dos sistemas híbridos porque são vulneráveis a mudanças de dados não atribuíveis.

5.6.9. Para todos os sistemas, três níveis diferentes devem, no mínimo, ser criados: administrador, supervisor e usuário ou operador. Alguns outros podem ser criados, se necessário. Os nomes dos grupos podem mudar de acordo com o aplicativo, por exemplo, analista no lugar de usuário e revisor para supervisor. Se o sistema não permitir 3 níveis, ele deve ser definido e documentado.

5.6.9.1 Administrador do sistema

5.6.9.1.1. O acesso do administrador do sistema deve ser restrito ao número mínimo de pessoas possível levando em consideração o tamanho, a natureza da empresa e o número de usuários para este sistema computadorizado específico. A conta genérica do administrador do sistema não deve estar disponível para uso. Os administradores de sistemas normalmente devem ser independentes dos usuários que realizam a tarefa e não ter envolvimento ou interesse no resultado dos dados gerados ou disponíveis no sistema eletrônico.

5.6.9.1.2. Onde o descrito acima não pode ser implementado devido à estrutura da empresa, um nível de controle semelhante pode ser alcançado pelo uso de contas duplicadas de usuário com privilégios diferentes. Todas as alterações realizadas no acesso do administrador do sistema devem ser transparentes e revisadas.

5.6.9.1.3. Um indivíduo deve fazer login usando a conta com os direitos de acesso apropriados para a determinada tarefa (ex. um coordenador de laboratório que executa a verificação de dados não deve fazer *login* como administrador do sistema quando existe um nível de acesso mais apropriado para essa tarefa).

5.6.9.1.4. As tarefas de administração do sistema devem ser identificadas, documentadas e suportadas através do controle de procedimentos. Os Administradores do Sistema devem ser treinados para executar essas tarefas e sua competência deve ser documentada e arquivada.

5.6.9.1.5. Quaisquer atividades relacionadas ao sistema que não são cobertas pelos procedimentos de administração padrão. Todas as atividades periódicas realizadas pelos Administradores devem ser documentadas em um protocolo ou *logbook*. As responsabilidades do administrador do sistema devem incluir:

5.6.9.1.6. Analisar os *logs* no sistema e identificar os problemas potenciais nos sistemas computadorizados;

5.6.9.1.7. Assegurar que as atualizações, os patches e as alterações de configuração do sistema operacional sejam aplicados;

5.6.9.1.8. Certificar que a instalação e configuração de novos *hardware* e *software* estão concluídas e foram documentadas.

5.6.9.1.9. Adicionar, remover ou atualizar informações de conta de usuário, redefinindo senhas, etc.

5.6.9.1.10. Criar e manter atualizada a lista de usuários para cada *software* ou equipamento. A listagem de usuários deve ter as páginas numeradas. Quando da necessidade, uma nova versão da listagem deve ser criada para a descrição dos novos usuários;

5.6.9.1.11. Atender consultas técnicas e auxiliar os usuários;

5.6.9.1.12. Manter a segurança do sistema ou equipamento (responsável);

5.6.9.1.13. Documentar a configuração do sistema;

5.6.9.1.14. Diagnosticar e reportar todos os problemas;

5.6.9.1.15. Assegurar que a infraestrutura de rede esteja funcionando. Caso necessário, aciona e supervisiona as atividades de TI ou do suporte técnico;

5.6.9.1.16. Configurar, adicionar e excluir arquivos do sistema (documentar);

5.6.9.1.17. Responsabilidade pela política de *backup* e restauração;

5.6.9.1.18. Atualizar os sistemas computadorizados através de Controle de Mudança. Quando essas atividades não são executadas pelo administrador do sistema, o mesmo tem a responsabilidade de acompanhar o executor, além de documentar a atividade e quaisquer riscos para a integridade dos dados no respectivo CM.

5.6.9.1.19. A identificação na trilha de auditoria de tentativas de acesso não autorizadas ao sistema deve ser comunicada ao proprietário do sistema.

5.6.9.20. Supervisor

5.6.9.2.1. O nível de acesso do supervisor pode modificar e criar métodos e relatórios, modificar configurações de instrumentos, assinar e aprovar protocolos, métodos e relatórios para sua utilização etc.

5.6.9.2.2. O supervisor pode ser responsável pela revisão da trilha de auditoria. Um supervisor não pode ter acesso ao gerenciamento de conta, configuração de trilha de auditoria e exclusão ou modificação de dados e não deve ter permissão para executar o processo com o acesso do supervisor.

5.6.9.3. Usuário

5.6.9.3.1. O nível de acesso do usuário permite a utilização do equipamento ou sistema para executar um processo. Ex. análise de amostras, embalagem, rotulagem e impressão.

5.6.9.3.2. Um usuário não pode ter acesso ao gerenciamento de conta, configuração de trilha de auditoria e exclusão ou modificação de dados. Caso necessite de acesso para modificar alguns dados, esta atividade deve ser documentada e verificada. Os usuários podem ter acesso somente leitura para a trilha de auditoria.

5.6.9.4. Usuários específicos

5.6.9.4.1. Contas de acesso temporário podem ser criadas como parte das atividades de qualificação/validação, nesses casos, as contas temporárias devem ser desativadas antes da liberação do sistema para uso.

5.6.9.4.2. Podem ser atribuídos níveis adicionais para cobrir funções como manutenção, engenharia e fornecedores.

5.6.9.4.2.1. Usuários de manutenção

5.6.9.4.2.1.1. Para usuários de manutenção, o perfil específico pode ser definido. Alguns instrumentos precisam de usuários de manutenção para executar a calibração, substituição de peças e testar o sistema computadorizado após o reparo.

5.6.9.4.2.1.2. As ações de manutenção exigem, por vezes, direitos de administrador no sistema. Se estes direitos forem necessários, isso deve estar descrito no procedimento e o treinamento adequado deve ser dado para explicar o impacto destes direitos sobre o sistema.

5.6.9.4.2.1.3. Se uma conta genérica for usada para manutenção, o nome do usuário e o período exato de tempo utilizado deve ser documentado no *logbook* do equipamento.

5.6.9.4.2.2. Usuários do fornecedor

5.6.9.4.2.2.1. Para suportar atividades periódicas como manutenção e qualificação, um nível de acesso individual ao usuário fornecedor pode ser configurado. Os fornecedores devem ter acesso ao equipamento ou ao *software*. Se uma conta genérica for usada para manutenção, o nome do usuário e o período exato de tempo utilizado deve ser documentado no *logbook* do equipamento.

****5.6.9.4.2.2.2. Todo o processo de intervenção remota deve estar descrito em análise de risco realizada durante a aquisição de um equipamento. O processo de acesso remoto para equipamentos standalone deverá estar descrito nos procedimentos de administração dos sistemas quando aplicável. O procedimento e aprovação de acesso externo (remoto) à rede deve seguir as políticas de TI. O suporte remoto de parceiros externos à rede deve ser identificado com uma conta externa criada pela área de TI para a empresa terceira. Essas contas devem ser claramente identificadas com pelo menos o nome da empresa e devem ser ativadas e desativadas antes e depois da intervenção.

5.6.9.4.2.2.3. Se houver um problema na ativação / desativação, um acompanhamento dedicado e regular do uso dessas contas deve ser feito (atividades periódicas) pelo administrador do sistema.

****5.6.9.4.2.2.4. Todas as contas padrão, incluindo contas de fornecedores e senhas, devem ser desativadas sempre que possível, e uma conta de fornecedor interno deve ser criada. A rastreabilidade das atividades do fornecedor (para contas internas de fornecedores e contas padrão de fornecedores que não podem ser desativadas) deve ser documentada para identificar quem (nome da empresa e técnico) realizou a atividade e quando.

5.6.9.4.2.2.5. Em situações em que as contas padrão de fornecedores e contas de acesso externo não podem ser desativadas, as tarefas realizadas com essas contas devem ser revistas como parte da revisão da trilha de auditoria.

## 5.7 Gerenciamento de Segurança

5.7.1. Os sistemas e dados computadorizados devem ser adequadamente protegidos contra perdas, danos ou alterações não autorizadas ou acidentais.

5.7.2. Os procedimentos para gerenciar o acesso seguro (incluindo a descrição do perfil dos usuários), adição e remoção de privilégios para usuários autorizados (por *Trilha de Auditoria*), gerenciamento de vírus, gerenciamento de senha, gerenciamento de patches e medidas de segurança física devem ser estabelecidos antes que o sistema seja aprovado para uso.

5.7.3. Um procedimento automatizado de captura de dados ou impressoras anexadas a equipamentos, tais como balanças, devem ser implementados antes que o sistema seja aprovado para uso.

5.7.4. É permitido o acesso a dados brutos para a equipe que realizará as atividades de verificação de dados. Os dados brutos devem ser acessados, mas qualquer alteração ou modificação deve ser rastreada ou restrita, mantendo o histórico de dados brutos e suportados por procedimentos locais necessários:

5.7.4.1. Seguir os procedimentos de gerenciamento de perdas para desautorizar eletronicamente tokens perdidos, roubados, faltantes ou potencialmente comprometidos, e outros dispositivos que carregam ou geram código de identificação ou informações de senha e emitir substituições temporárias ou permanentes usando controles adequados e rigorosos.

5.7.4.2. Se possível, as tentativas não autorizadas de acesso a sistemas informatizados devem ser registradas na Trilha de Auditoria e informadas ao administrador para investigação. Procedimentos para rever a trilha Auditoria periodicamente procurando tentativas não autorizadas devem ser implementadas. Durante a trilha de auditoria, recomenda-se confirmar que o perfil do usuário esteja corretamente configurado para a solicitação de conta relacionada.

5.7.4.3. Testes iniciais e periódicos de dispositivos, como tokens ou cartões, que carregam ou geram códigos de identificação ou informações de senha para garantir que eles funcionam corretamente e não tenham sido alterados de forma não autorizada.

5.7.4.5. Os procedimentos para gerenciar a criação, alteração e cancelamento de autorizações de acesso devem ser implementados e, quando possível, essas alterações devem ser registradas pelo aplicativo.

5.7.4.6. Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade de operadores que entram, mudam, confirmam ou excluem dados, incluindo data e hora.

5.7.4.7. O suporte de instalação (CD, DVD, documentação de instalação e configuração) deve ser armazenado em locais protegidos com acesso limitado e protegidos do fogo e da água.

****

5.8 Acesso ao gerenciamento de data e hora

5.8.1 Para registrar eventos cronometrados corretamente, todos os sistemas devem ter relógios controlados/sincronizados adequadamente. Isso significa que os relógios do sistema devem ser conectados a um servidor NTP qualificado. Se a sincronização não for possível, a data e hora deve ser verificada periodicamente e comparado com o relógio de referência (horas e minutos). Os relógios do sistema local devem ser configurados para o fuso horário correto, incluindo o horário de verão em um formato de data/hora inequívoco (quando possível é recomendado seguir o formato DD-MM-YYYY). Em geral, a diferença de tempo de até 5 minutos pode ser aceitável, sistemas de alto risco podem definir uma diferença de tempo aceitável mais curta. Uma diferença de tempo mais aceitável pode ser justificada com uma avaliação de risco. O ajuste manual do tempo no SC precisa ser registrado e justificado no Logbook do SC ou no próprio SC se essa funcionalidade estiver disponível. Somente os administradores terão acesso aos parâmetros do sistema, gerenciamento da conta, mudança de data e horário, incluindo parâmetros de fuso horário e horário.

# 6. Referências

• RDC 430 Nº 430/2020 (ANVISA) - Dispõe sobre as Boas Práticas de Distribuição, Armazenagem e de Transporte de Medicamentos;

• Guia de Validação de Sistemas Computadorizados nº 33/2020, 1ª Versão ANVISA,

• GAMP5, PIC/S, 21 CFR Part 11.

# 7. Histórico

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA** | **REVISÃO** | **DESCRIÇÃO DA ALTERAÇÃO** | **OBSERVAÇÃO** |
| 05/04/2024 | 000 | Criação | N/A |

# 8. VALIDAÇÃO

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaborado por:** | **Tatiana Gonçalves**  Responsável |  | 05/04/2024 |
| **Revisado por:** | **XXXXXXXX**  Coordenador Operacional |  | XX/XX/XXXX |
| **Aprovado por:** | **XXXXXXX**  Gerente Operacional |  | XX/XX/XXX |

# 9. Anexos

Não aplicável.