Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	20/10/2025	Igo	Criação da Política	Ageu

Sumário

1. Propósito e Escopo

Esta Política de Gestão de Acessos (PGA) tem como propósito complementar as diretrizes de Segurança da Informação, estabelecendo os mecanismos de controle de identificação, autenticação e autorização para salvaguardar as informações e ativos do Hospital, com o objetivo de proteger os Dados Pessoais Sensíveis e evitar acessos não autorizados que impliquem em risco de perda, destruição ou divulgação indevida.

Esta PGA abrange a gestão de acessos lógicos (sistemas, redes, recursos de TI) e físicos (instalações, salas críticas).

2. Princípios e Modelos de Acesso

O controle de acesso no Hospital será orientado por dois princípios primários e um modelo de gestão:

a) **Princípio do Menor Privilégio (Privilégio Mínimo):** Os usuários terão acesso apenas aos recursos e informações estritamente necessários para o desempenho de suas funções.
b) **Princípio da Necessidade de Conhecimento (Need-to-Know):** O acesso a informações confidenciais e restritas, como prontuários, deve ser configurado apenas quando houver uma necessidade de trabalho identificada e o acesso for aprovado pelo Proprietário da Informação.
c) **Modelo de Acesso Baseado em Funções (RBAC):** O controle de acesso será implementado e mantido com base nas funções/papéis (ou perfis) dos colaboradores.

3. Identificação e Autorização

3.1. Definição de Privilégios

A Equipe de Segurança da Informação, em conjunto com os Proprietários da Informação (Gestores das áreas), é responsável por:

a) Definir os perfis de acesso (privilégios) com base nas tarefas, alinhando-os ao nível de classificação da informação (PÚBLICA, INTERNA, RESTRITA, CONFIDENCIAL) definido na Política de Classificação da Informação (PCI).

b) Elaborar e manter a documentação dos direitos de acesso para cada função dentro do Hospital.

c) Ao conceder acesso a usuários que lidam com Dados Pessoais Sensíveis, limitar estritamente o acesso ao mínimo necessário para cumprir os objetivos essenciais do processamento (Minimização de Dados).

3.2. Contas de Acesso e Provisionamento

A gestão adequada das contas de acesso é fundamental para mitigar riscos e assegurar que apenas usuários autorizados acessem os sistemas. Para isso, aplicam-se as seguintes regras:

a) **Identificador Único:** Cada usuário deve possuir uma identificação (login) exclusiva e única.

b) **Contas de Serviço:** Contas de serviço (necessárias a um procedimento automático) devem ser inventariadas e gerenciadas, sendo utilizada uma credencial específica para este propósito.

c) **Contas Privilegiadas (Administradores):** Usuários com privilégios administrativos devem possuir uma credencial específica e dedicada exclusivamente para a execução de atividades administrativas. Esta credencial privilegiada não deve ser utilizada para atividades gerais como navegação na internet ou e-mail.

d) **Inventário e Revisão:** Um inventário centralizado de todas as contas (usuário, administrativas, de serviço) deve ser estabelecido e mantido atualizado. As contas ativas devem ser validadas periodicamente (ex: a cada 90 dias, conforme sugerido em modelos de boas práticas).

4. Gestão de Credenciais e Autenticação

Esta seção estabelece as diretrizes para a criação, uso e gestão das credenciais de acesso lógico, visando garantir a autenticidade dos usuários e proteger os ativos de informação.

4.1. Controle de Senhas

As diretrizes para senhas devem ser rigorosamente seguidas para minimizar pontos de vulnerabilidade, sendo que as vulnerabilidades de senha são consideradas as principais causadoras de ataques cibernéticos. Sendo assim, ficam estabelecidos os seguintes critérios técnicos e comportamentais para todas as senhas de acesso utilizadas no ambiente corporativo:

a) **Requisitos Mínimos de Força:** A senha de acesso deve ter um tamanho mínimo de 12 (doze) caracteres, composta obrigatoriamente por uma combinação de:
   i) Letras maiúsculas e minúsculas.
   ii) Números.
   iii) Caracteres especiais (ex: !, $, #, %).

b) **Inicialização:** A senha inicial é temporária e deve ser obrigatoriamente alterada no primeiro acesso.

c) **Histórico de Reutilização:** Não é permitido o uso das últimas 3 (três) senhas utilizadas.

d) **Proibições:** É proibido o uso de informações pessoais óbvias (como nomes, datas de nascimento ou informações facilmente acessíveis) na criação de senha. Também não devem ser utilizados termos óbvios como "senha", "usuário", "password" ou "system".

e) **Bloqueio por Tentativas:** A conta de acesso será bloqueada automaticamente após 5 (cinco) tentativas consecutivas de acesso inválido.

f) **Sigilo e Compartilhamento:** O login e a senha são de uso pessoal e intransferível. É proibida sua divulgação ou compartilhamento, sendo o empréstimo de credenciais considerado infração disciplinar grave.

g) **Armazenamento Seguro:** É estritamente proibido manter senhas registradas em arquivos na rede, no computador, em anotações ou qualquer outro meio que comprometa o sigilo.

4.2. Autenticação Multifator (MFA)

O MFA (Autenticação de Multifatores) deve ser implementado para reforçar a autenticação de identidade.

a) **Obrigatoriedade de Uso:** A Autenticação de Multifatores (MFA) deve ser utilizada sempre que possível, sendo obrigatória para:
   i. Acesso remoto via VPN (Rede Virtual Privada). O acesso remoto deve ser controlado por autenticação forte, de preferência com MFA.
   ii. Todas as contas com privilégio administrativo.
   iii. Acesso a todas as aplicações corporativas ou de terceiros hospedadas em fornecedores.

b) **Biometria:** Quando implementada, a conta de acesso biométrico deve ser vinculada a uma conta de acesso lógico (login/senha) para atender os conceitos da MFA. Os dados biométricos devem ser tratados como sigilosos, utilizando preferencialmente criptografia.

5. Desprovisionamento e Revogação (Gestão do Ciclo de Vida do Acesso)

A revogação de acessos deve ser imediata em caso de encerramento de vínculo, para mitigar o risco de acessos indevidos por ex-colaboradores.

Este princípio de remoção imediata se aplica não apenas a desligamentos, mas também a mudanças de função e períodos de inatividade. Sendo assim, o processo de desprovisionamento e revogação seguirá as seguintes regras:

a) **Desligamento e Revogação Imediata:** Os direitos de acesso (lógicos e crachás) devem ser imediatamente removidos ou desabilitados após

o encerramento das atividades, contratos ou desligamento do usuário. O acesso de ex-servidores ou ex-contratados aos sistemas de informação deve ser proibido.

b) **Comunicação Imediata (RH):** A área de Recursos Humanos (RH) é responsável por comunicar imediatamente à área de TI sobre desligamentos, férias, licenças, transferências e modificações no quadro de colaboradores. A TI deve realizar os ajustes ou a desativação do perfil de acesso em até 2 horas após o registro do chamado de desligamento pelo RH.
c) **Movimentação Interna:** Em caso de mudança de função ou setor, os direitos de acesso antigos devem ser imediatamente revogados, e novos acessos concedidos conforme a nova função.
d) **Inatividade:** Contas ativas e sem atividade por mais de 45 (quarenta e cinco) dias poderão ser automaticamente bloqueadas sem aviso prévio. Contas não utilizadas há mais de 180 (cento e oitenta) dias poderão ser canceladas.
e) **Bloqueio de Sessão:** O bloqueio automático de sessão nos ativos de TI deve ser configurado após um período de inatividade preestabelecido (ex: 15 minutos), exigindo nova autenticação para evitar acesso de terceiros a dados confidenciais.
f) **Priorização:** A TI deve priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

6. Controle de Acesso Físico

A segurança da informação não se limita ao ambiente digital. A proteção dos ativos de informação e da infraestrutura de TI depende diretamente da implementação de controles de acesso físico para proteger os locais onde os dados são armazenados, processados ou acessados.

Para mitigar riscos de intrusão, danos ou acesso indevido a Dados Pessoas Sensíveis (como prontuários em arquivos físicos ou servidores), aplicam-se os seguintes controles:

a) **Perímetros de Segurança:** O Hospital deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências.
b) **Ambientes Seguros:** Áreas críticas (como Salas de Servidores/CTI, Salas de Arquivo Médico, Farmácia Hospitalar) devem ser protegidas por mecanismos de controle de acesso (fechaduras digitais, biometria, cartões de acesso).
c) **Monitoramento:** Os mecanismos de controle de acesso devem ser monitorados pelo Setor de Segurança.
d) **Acesso de Terceiros:** O acesso a ambientes seguros por fornecedores ou prestadores de serviços será concedido somente para fins específicos e autorizados, devendo ser supervisionado e monitorado.
e) **Logs de Acesso:** O Hospital deve manter um log ou registro físico seguro de todos os acessos aos ativos de informação.

7. Monitoramento, Treinamento e Conformidade

7.1. Monitoramento e Auditoria

A simples implementação de controles de acesso não garante a segurança. É essencial verificar ativamente se esses controles estão sendo utilizados corretamente e se há tentativas de burlá-los. Para isso, o Hospital manterá um processo contínuo de monitoramento e auditoria focado na detecção e resposta a anomalias, com base nas seguintes ações:

a) **Registro de Atividades:** As atividades de acesso dos usuários (lógico e físico) devem ser registradas e monitoradas continuamente para detectar atividades suspeitas ou não autorizadas.

b) **Análise de Logs:** Devem ser realizadas análises dos registros de atividades para identificar padrões incomuns ou atividades suspeitas.
c) **Integração de Sistemas:** Assegurar a integração entre controle de acesso, CFTV (vídeo monitoramento) e sistemas de gestão de RH para uma resposta coordenada a incidentes.

7.2. Treinamento

O fator humano é uma prioridade, visto que muitas falhas ocorrem por descuidos humanos.

a) **Capacitação:** Programas de treinamento e conscientização regulares são obrigatórios, abordando temas como a LGPD, o uso ético de dados clínicos e a confidencialidade.
b) **Engajamento:** O treinamento deve focar na conscientização contínua sobre a importância da segurança, incluindo os riscos e consequências do não cumprimento das políticas de acesso.

8. Responsabilidades e Penalidades

A eficácia dos controles de acesso depende do correto cumprimento desta política por todos os usuários. Sendo assim, ficam estabelecidas as responsabilidades individuais e as consequências administrativas, civis e criminais aplicáveis em caso de descumprimento:

a) **Responsabilidade do Usuário:** O usuário é responsável por todos os acessos realizados através de sua conta, devendo interromper a conexão ou bloquear o equipamento ao se ausentar do local de trabalho.
b) **Incidentes:** Qualquer utilização não autorizada ou tentativa de utilização de credenciais será tratada como um incidente de segurança da informação.

c) **Sanções:** O não cumprimento desta Política implica em falta grave, sendo passível de penalidades (advertências, rescisão contratual) e/ou responsabilidade civil e criminal, conforme a legislação vigente (LGPD).

d) **Suspensão de Serviço:** Em caso de suspeita de quebra da segurança da informação, a Equipe de Segurança da Informação conduzirá a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.