HOSPITAL
SÃO MARCOS

Política de Gestão e Controle de Acesso

HOSPITAL SÃO MARCOS

Sumário

HOSPITAL
SÃO MARCOS

1. Visão Geral

O Departamento de Segurança da Informação publica esta política com o objetivo de estabelecer e manter normas e controles eficazes relacionados ao acesso aos ativos e sistemas de informação do Hospital São Marcos. Esta política visa garantir que o acesso a informações seja devidamente autorizado, monitorado e revogado, de modo a proteger a confidencialidade, integridade e disponibilidade das informações da organização.

2. Objetivo

Esta política tem como objetivo estabelecer diretrizes para o controle e a gestão dos acessos lógicos aos ativos e sistemas de informação do Hospital São Marcos, assegurando que todos os acessos sejam concedidos, utilizados e monitorados de forma segura, de acordo com as necessidades do negócio e com os requisitos da norma ISO/IEC 27001.

3. Escopo

Aplica-se a todos os colaboradores, terceiros, estagiários e prestadores de serviço que utilizem os ativos de tecnologia do Hospital São Marcos, incluindo, mas não se limitando a: rede local, rede sem fio, internet, intranet, sistemas de informação, dispositivos móveis, estações de trabalho e serviços em nuvem.

4. Definições

- **Sistemas da Informação:** Qualquer aplicação, sistema ou infraestrutura tecnológica utilizada para processar, armazenar ou transmitir informações organizacionais, incluindo: servidores, banco de dados, correio eletrônico, intranet, ERP, CRM, entre outros.

- **Inventário de Gestão de Acessos:** Documento ou sistema de controle que registra todas as contas criadas, alteradas, bloqueadas ou excluídas, bem como seus respectivos níveis de acesso, perfis e permissões.

- **Princípio do Menor Privilégio:** O acesso concedido ao usuário deve ser o mínimo necessário para o desempenho de suas funções.

- **Autenticação Multifator (MFA):** Recurso adicional de autenticação que combina duas ou mais credenciais independentes (ex.: senha + token ou biometria).
- **Acesso Genérico:** Conta de uso compartilhado entre vários usuários (permitida apenas sob exceção formal aprovada).

5. Diretrizes

A Gestão de Acessos é essencial para manter controles de acesso rigorosos. Este tópico detalha os procedimentos para conceder, revisar e revogar acessos, assegurando que apenas usuários autorizados possam acessar os recursos do Hospital São Marcos.

5.1 Controle de Acesso Físico

O acesso às dependências físicas do Hospital São Marcos deve ser rigorosamente controlado, de modo a proteger pessoas, informações e ativos contra acessos não autorizados, danos, interferências ou furtos.

Entre as medidas implementadas, destacam-se:

- Controle de acesso às áreas restritas, por meio de dispositivos eletrônicos, biometria ou chaves de acesso individuais;
- Uso obrigatório de crachá de identificação por todos os colaboradores, prestadores de serviço, visitantes e terceiros, de forma visível durante toda a permanência nas dependências do hospital;
- Acompanhamento e registro de visitantes;
- Monitoramento contínuo por sistemas de CFTV, com câmeras instaladas em pontos estratégicos para vigilância das áreas internas e externas;
- Sistemas de alarme e detecção de intrusão, instalados nas áreas de maior criticidade.

5.2 Controle de Acesso Lógico

- **Autenticação:** Todos os usuários devem utilizar credenciais únicas, e a autenticação multifator (MFA) deve ser implementada sempre que possível.

- **Autorização:** O acesso aos sistemas e dados devem ser controlados por meio de listas de controle de acesso e políticas de grupo.

- Não são permitidas contas de acesso genéricas aos sistemas da informação, salvo em casos excepcionais devidamente justificados, documentados e autorizados pela área de Segurança da Informação e com a aprovação da alta direção.

- **Gerenciamento de Senhas:** Devem ser aplicadas políticas rigorosas de senhas, incluindo complexidade mínima, validade e histórico de senhas.

- **Controle de Acesso Baseado em Função (RBAC):** A atribuição de permissões deve ser realizada com base nas funções dos usuários, garantindo que cada um tenha acesso apenas às informações necessárias para suas atividades.

5.3 Segregação de Funções

Atribuições conflitantes devem ser segregadas para evitar que um único indivíduo tenha controle total sobre processos críticos.

5.4 Solicitação de Acesso

Toda solicitação de criação, alteração ou revogação de acesso deve ser formalizada pelo gestor do usuário por e-mail ou formulário específico. A solicitação deve conter:

- Nome completo e matrícula do colaborador;
- Sistema(s) para o qual o acesso é solicitado;
- Perfil ou grupo de acesso requerido;
- Justificativa do acesso.

A criação de contas deve seguir o padrão corporativo definido: primeiro nome e último sobrenome do colaborador (exemplo: joaosilva).

5.5 Revogação de Acesso

A revogação de acessos ocorre de forma automática em casos de desligamento do colaborador ou mediante solicitação do gestor.

Quando o colaborador é removido da folha de pagamento, uma rotina automatizada, executada diariamente, identifica o desligamento e realiza a revogação dos acessos de forma imediata.

5.6 Inventário de Acessos

Todos os acessos concedidos ou alterados devem ser registrados no Inventário de Gestão de Acessos, contendo:

- Data de criação;
- Modificações de permissões;
- Data de revogação/exclusão;
- Responsável pela aprovação.

Periodicamente deve ser realizada a verificação das permissões de contas de acesso aos sistemas da informação no Inventário de Gestão de Acesso, com o intuito de prevenir permissões em excesso, contas ativas de colaboradores já desligados, não cumprimentos das políticas da organização, entre outros.

5.7 Revisão de Acessos

A revisão dos acessos deve ser realizada trimestralmente, para garantir que todos os acessos estejam atualizados e em conformidade com as políticas de segurança do Hospital São Marcos.

5.8 Termo de Responsabilidade

Todos os colaboradores, clientes e parceiros que possuírem contas de acesso aos sistemas de informação do Hospital São Marcos devem assinar o Termo de Responsabilidade, bem como as políticas vigentes de Segurança da Informação.

Além disso, todos os colaboradores que manusearem informações do Hospital São Marcos devem assinar o Termo de Confidencialidade e Não Divulgação (NDA) no momento de sua admissão.

6. Papéis e Responsabilidades

- **Equipe de Segurança da Informação:** Definir e orientar sobre os procedimentos relacionados.

- **Equipe de TI:** Implementar, manter e monitorar os sistemas de controle de acesso.
- **Colaboradores:** Cumprir as diretrizes desta política e reportar qualquer incidente de segurança.

7. Conformidade da Política

7.1 Gestão de Conformidade

O Departamento de Segurança da Informação será responsável por verificar e monitorar a conformidade com esta política por meio de diversos métodos, incluindo auditorias internas e relatórios de ferramentas, para garantir que as práticas e controles de segurança sejam seguidos corretamente.

7.2 Exceções

Qualquer exceção a esta política deve ser previamente autorizada pelo Departamento de Segurança da Informação e devidamente documentada.

7.3 Não Conformidade

Caso sejam encontradas violações a esta política, poderão ser aplicadas ações disciplinares, incluindo advertências, demissão, e, quando aplicável, a adoção de medidas jurídicas conforme a gravidade da infração.

7.4 Atualização da Política

Está política deve ser revisada anualmente, ou sempre que houver mudanças significativas nos processos envolvidos.

8. Histórico de Revisão

Data de alteração	Responsável	Atualização
03/05/2022	Vivyan Caroline	Criação da Política.
02/07/2025	Nathali Macedo	Revisão da Política.