Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	08/10/2025	Ageu	Criação da Política	Samuel
2	22/10/2025	Larissa	Aumento do número de caracteres na senha	Igo

Sumário

1. Objetivo

O objetivo desta política é estabelecer regras e diretrizes para o uso adequado e seguro de todos os recursos de Tecnologia da Informação do Hospital, visando proteger a infraestrutura, a informação (especialmente Dados Pessoais Sensíveis de pacientes e colaboradores) e garantir a conformidade legal.

2. Regras Gerais para uso da Rede Corporativa e Equipamentos

Esta seção estabelece as diretrizes fundamentais para acesso e segurança geral na infraestrutura de TI do Hospital.

2.1. Acesso e Contas de Usuário

a) **Restrição de Acesso:** O acesso à rede é permitido exclusivamente a pessoas explicitamente autorizadas e limitado ao mínimo necessário para o desempenho de suas funções (Princípio do Mínimo Acesso).

b) **Identificação Pessoal:** Cada usuário deve possuir uma identificação (login) exclusiva, sendo seu uso pessoal e intransferível. O empréstimo de credenciais é considerado infração disciplinar grave.

c) **Gestão de Contas:**

i) Contas ativas e sem atividade por mais de 45 dias, não havendo justificativa válida, serão automaticamente bloqueadas sem aviso prévio.

ii) Em casos de desligamento, mudança de função ou fim de contrato, o RH deve registrar um chamado para que a TI realize os ajustes ou a desativação do perfil de acesso em até 2 horas após o registro.

2.2. Política de Senha Obrigatória

a) **Sigilo:** A senha é pessoal e intransferível, devendo ser mantida em total sigilo.

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

c) **Requisitos Mínimos:** A senha deve ter um tamanho mínimo de 12
d) caracteres, composta por letras (maiúsculas e minúsculas), números e caracteres especiais (ex: !, $, #, %).
e) **Atualização:** Será solicitada automaticamente a alteração da senha a cada 60 dias.
f) **Histórico:** Não é permitido o uso das últimas 3 (três) senhas utilizadas.
g) **Bloqueio:** A conta de acesso será bloqueada automaticamente após 5 tentativas inválidas. Caso o usuário não consiga acessar sua conta, deverá solicitar o desbloqueio ou redefinição de senha junto à equipe de suporte técnico, exclusivamente por meio dos canais autorizados. A identidade do solicitante será validada antes da liberação do acesso.
h) **Armazenamento:** É proibido manter senhas registradas em arquivos na rede, no computador, em anotações ou qualquer outro meio que comprometa o sigilo.

2.3. Monitoramento, Uso e Responsabilidade

a) **Monitoramento:** A Instituição e/ou o Setor de TI se reservam o direito de monitorar e gravar todo o uso da rede corporativa, Internet, e-mail e estações de trabalho. Os dados de uso podem ser auditados via logs de sistemas.
b) **Uso Profissional:** Os recursos computacionais são propriedade do Hospital LISA e devem ser utilizados exclusivamente para a atividade profissional e para os objetivos da Instituição.
c) **Bloqueio de Inatividade:** Após 15 minutos de inatividade, a tela do equipamento será bloqueada, exigindo nova autenticação para evitar acesso de terceiros a dados confidenciais ou sensíveis.
d) **Responsabilidade por Danos:** Qualquer dano ou prejuízo material ou informacional causado por mau uso ou negligência na guarda dos equipamentos e credenciais será de inteira responsabilidade do colaborador.

2.4. Uso de Impressoras e Scanners

a) **Finalidade:** Devem ser utilizados única e exclusivamente para atender às necessidades do Hospital LISA.
b) **Proibições:** É proibida a impressão de documentos particulares ou a utilização das funcionalidades de scan/cópia para materiais que violem Direitos Autorais.
c) **Segurança da Informação:** O colaborador deve certificar-se de que a impressão esteja segura e seja imediatamente recolhida para evitar o vazamento de informações e dados confidenciais ou sensíveis.
d) **Auditoria:** O conteúdo impresso e escaneado poderá ser monitorado.

3. Regras para uso de e-mail Corporativo

O e-mail é uma ferramenta corporativa e seu uso deve refletir o profissionalismo e as normas de segurança da informação da Instituição.

3.1. Uso e Conduta Profissional

a) **Exclusividade:** O e-mail deve ser utilizado única e exclusivamente para o trato de questões de interesse da Instituição.
b) **Proibição de Uso Pessoal:** Não pode ser utilizado para fins pessoais ou que infrinjam o Código de Ética da Instituição.
c) **Individualidade:** A conta é individual, e o colaborador é responsável por toda mensagem enviada a partir de seu endereço, devendo zelar pela imagem da organização e utilizar linguagem profissional.
d) **Transferência:** A conta de e-mail não pode ser transferida ou cedida a terceiros.

3.2. Segurança e Conteúdo Proibido

a) **Conteúdo Ofensivo/Ilegal:** É proibido o uso para transmitir/divulgar material ilegal, difamatório, abusivo, ameaçador, obsceno, ou que viole a privacidade de terceiros.
b) **Imagens Corporativas/Éticas:** É proibido o uso de e-mail que contenha declarações com ideologias políticas, religiosas, raciais, pornografia, apologia às drogas ou que possam prejudicar a imagem da organização, pacientes, concorrentes ou fornecedores.
c) **Compartilhamento de Dados:**
    i) Não compartilhar Dados Pessoais e Dados Pessoais Sensíveis (exames, laudos, histórico de saúde) via e-mail.
    ii) Caso estritamente necessário e autorizado, o usuário deve certificar-se de que os destinatários seguem a Política de Privacidade de Dados, atendendo à LGPD.

3.3. Propriedade e Auditoria de E-mail

a) **Propriedade Institucional:** Todos os e-mails recebidos ou enviados através da conta corporativa são de propriedade do Hospital LISA.
b) **Monitoramento:** Todos os e-mails estão sujeitos ao monitoramento integral de seu conteúdo, a qualquer momento e sem notificação prévia.
c) **Gestão de Conteúdo:** O usuário não deve esvaziar a caixa de e-mail ou eliminar arquivos em caso de afastamento ou desligamento, visto que o conteúdo pertence à instituição.
d) **Acesso Restrito:** O acesso a e-mails de colaboradores desligados ou afastados é restrito, exigindo aprovação formal da gerência.

4. Regras Para Uso de Internet

O acesso à Internet é um recurso profissional e deve ser gerido para manter a produtividade e a segurança da rede.

4.1. Finalidade e Controle de Acesso

a) **Aderência:** O acesso à Internet é permitido se for aderente aos objetivos e atividades fins desempenhadas pelo usuário (uso profissional).
b) **Sites Proibidos:** Sites com conteúdo pornográfico, de apologia ao racismo/discriminação, de jogos online, ou de relacionamento não devem ser acessados. A TI utilizará filtros de acesso para bloquear esta navegação.
c) **Exceções:** Se for necessário o acesso a sites bloqueados por motivos estritamente profissionais, o usuário deverá solicitar a liberação via chamado, que será analisado pela TI e aprovado formalmente pela gerência.
d) **Relatórios:** O sistema de filtros de acesso pode gerar relatórios periódicos para auditoria do uso.

4.2. Conteúdo e Software

a) **Download Proibido:** É estritamente proibido fazer download de software comercial ou material protegido por Direitos Autorais (copyright) sem um contrato de licenciamento válido. É proibido baixar programas de entretenimento ou jogos.
b) **Vírus e Malware:** Nenhum usuário pode utilizar os recursos para deliberadamente propagar qualquer tipo de vírus ou programas de controle de outros computadores.
c) **Instalação de Programas:** É proibido instalar programas provenientes da Internet ou de qualquer outra fonte sem expressa autorização do Departamento de TI.

d) **Redes P2P e Mensageiros:** É proibido o uso de ferramentas P2P, P2M e de Redes Sociais ou Instant Messenger (IM) não autorizados para fins profissionais ou pessoais.

5. Regras Para Dispositivos Móveis e Mídias Removíveis

Esta seção trata do risco de vazamento de dados via dispositivos não corporativos e mídias físicas.

5.1. Uso de Mídias Removíveis (USB, Pen Drive, etc.)

a) **Bloqueio Padrão:** O uso de mídias removíveis é considerado uma fonte de infecção por malwares e um risco de evasão de dados. As portas de comunicação USB e barramentos similares (bluetooth) são automaticamente bloqueadas por software de gerenciamento central.
b) **Concessão Excepcional:** Para concessão de acesso (excepcional), é necessário registrar um chamado, anexar um termo de autorização específico e ter aprovação formal do gestor.
c) **Termo de Responsabilidade:** O usuário e o gestor assinam um termo de responsabilidade, assumindo a inteira e exclusiva responsabilidade por manter a integridade, confidencialidade e disponibilidade dos dados do Hospital.

5.2. Dispositivos Móveis (Smartphones e Tablets Corporativos/Pessoais)

a) **Equipamentos Corporativos:** Usuários que utilizam smartphones/tablets fornecidos pelo Hospital devem assinar o respectivo termo de responsabilidade. É vedado o uso do equipamento para qualquer finalidade que não seja ligada diretamente às atividades de sua área.
b) **Perda ou Roubo:** Em caso de perda ou roubo de equipamentos corporativos, o usuário deve formalizar imediatamente um Boletim de Ocorrência (BO) e comunicar o suporte da TI.

c) **Dispositivos Pessoais (BYOD - Bring Your Own Device):** O uso de dispositivos móveis pessoais não é autorizado para tratar de temas corporativos, especialmente Dados Pessoais e Dados Pessoais Sensíveis.

5.3. Uso de Aplicativos de Comunicação para Fins Profissionais

Se o uso for autorizado ou necessário:

a) **Prevenção de Vazamento:** O usuário deve evitar compartilhar Dados Pessoais/Sensíveis (exames, laudos, imagens) por esses meios.
b) **Minimização de Risco:** Caso estritamente necessário, deve-se adotar o envio de mensagens temporárias ou eliminar o conteúdo o mais breve possível do dispositivo após a inserção nos sistemas de gestão da organização (preferencialmente em até 24h).
c) **Corresponsabilidade:** O usuário está ciente de que o compartilhamento de Dados Pessoais/Sensíveis referente ao Hospital implica em corresponsabilidade jurídica sobre o dado.

5.4. Boas Práticas de Segurança

Recomenda-se que todos os dispositivos (corporativos ou pessoais autorizados) utilizem:

a) Software antivírus licenciado e atualizado.
b) Sistemas operacionais atualizados.
c) Senhas seguras (12 caracteres alfanuméricos) e bloqueio de tela automático.
d) Autenticação de dois fatores ativada (se suportado).
e) Criptografia de disco/dados.
f) Proibição de uso de Wi-Fi aberto (público) ou carregadores USB públicos para acessar dados hospitalares.

6. Conclusões e Penalidades

O não cumprimento de qualquer diretriz estabelecida nesta Política será considerado uma infração e estará sujeito a medidas disciplinares, que podem variar desde uma advertência até a rescisão do contrato de trabalho por justa causa, além de responsabilização civil e criminal, conforme a legislação vigente (incluindo a LGPD).