**OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

A Política de Segurança da Informação no contexto hospitalar tem como objetivo estabelecer normas, diretrizes e procedimentos que garantam a segurança das informações, sem prejudicar ou dificultar os processos essenciais da instituição, mas assegurando:

* **Confiabilidade das Informações:** Preservar a confidencialidade, integridade e disponibilidade dos dados relacionados ao atendimento médico, registros dos pacientes, informações clínicas e demais dados sensíveis, mantendo a qualidade e precisão das informações.
* **Compromisso do Hospital com a Proteção das Informações:** Reforçar o compromisso da instituição hospitalar com a proteção das informações sob sua responsabilidade, incluindo aquelas de propriedade do hospital e as que estão sob sua guarda, como registros médicos, dados administrativos e informações relacionadas à pesquisa clínica.
* **Participação e Cumprimento por Todos os Colaboradores no Processo:** Envolver todos os colaboradores, desde profissionais de saúde até funcionários administrativos, na adesão e cumprimento das práticas estabelecidas pela política, garantindo a segurança da informação em todas as fases do processo, desde a coleta até o arquivamento.

**CLASSIFICAÇÃO DAS INFORMAÇÕES**

As informações no contexto hospitalar devem ser devidamente classificadas e identificadas por rótulos, levando em consideração os seguintes níveis:

**Pública:**

São informações explicitamente aprovadas por seus responsáveis para consulta irrestrita.

A divulgação externa não compromete o negócio, e, portanto, não requer proteção específica.

Exemplos de informações públicas no ambiente hospitalar incluem editais de licitação, rotinas e agendas médicas, campanhas de promoção à saúde.

**Interna:**

São informações disponíveis aos colaboradores do hospital para a execução de suas tarefas rotineiras.

Não se destinam ao uso do público externo.

Exemplos de informações internas abrangem memorandos, portarias, padrões, políticas e procedimentos internos, e-mails e lista telefônica internos, avisos e campanhas internas.

**Confidencial:**

São informações de acesso restrito a colaboradores específicos.

A revelação dessas informações podem violar a privacidade de indivíduos, infringir acordos de confidencialidade, entre outros.

Exemplos de informações confidenciais em um ambiente hospitalar incluem exames e diagnósticos de pacientes, processos judiciais e dados cadastrais de funcionários.

Essa classificação visa garantir a proteção adequada das informações sensíveis, especialmente aquelas relacionadas à saúde dos pacientes, e assegurar que apenas pessoal autorizado tenha acesso a dados confidenciais. Essa abordagem busca equilibrar a transparência necessária para determinadas informações com a necessidade de preservar a privacidade e a segurança dos dados no ambiente hospitalar.

**POLÍTICA DE SENHAS**

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1) A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesmo ser imediatamente alterada no caso de suspeita de sua divulgação;

2) A senha inicial só será fornecida ao próprio colaborador, pessoalmente. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;

3) É proibido o compartilhamento de login para funções de administração de sistemas;

4) As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor etc.);

5) As senhas deverão seguir os seguintes pré-requisitos: - Tamanho mínimo de oito caracteres; - Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;

- Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge etc.).

6) O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

- Desligamento do colaborador;

- Mudança de função do colaborador;

- Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

**BACKUP**

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer. Assim, estabelecem-se as regras:

1) Todo sistema ou informação relevante para a operação dos negócios do Hospital deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;

2) As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e provocar o TI sobre a necessidade de backup deles, sugerindo o tempo de retenção destas cópias;

3) Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;

4) As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter;

5) Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;

6) O setor de TI deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;

7) Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade

**USO DAS ESTAÇÕES DE TRABALHO**

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

1) É de responsabilidade do colaborador do equipamento zelar por ele, mantendo-o em boas condições;

2) Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;

3) É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe do SGPTI;

4) As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas.

5) É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe do SGPTI;

6) É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe do setor de TI;

7) As estações de trabalho devem permanecer bloqueadas (logoff ) nos períodos de ausência do colaborador;

8) Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;

9) Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;

10) É proibido o uso de estações de trabalho para: - Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

- Burlar quaisquer sistemas de segurança;

- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

11) O setor de TI não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição;

12) As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário

**VIOLAÇÃO DA POLÍTICA E PENALIDADES**

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

- Advertência verbal O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação do HU-UFPI e será recomendado à leitura desta Norma;

- Advertência formal A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida. A segunda notificação será encaminhada para a chefia imediata do infrator

**CONTROLE DE PRIVILÉGIOS E CONTROLE DE ACESSOS**

Para fortalecer ainda mais a segurança da informação, é essencial implementar controles rigorosos de privilégios e acessos. Estes controles visam garantir que apenas usuários autorizados tenham acesso a informações específicas, reduzindo assim os riscos de vazamento ou manipulação indevida de dados.

**Controle de Privilégios:**

**Princípio do Privilégio Mínimo:** Os colaboradores devem receber apenas os privilégios necessários para realizar suas funções. O acesso a informações confidenciais deve ser restrito ao mínimo necessário para a execução das tarefas.

**Revisão Periódica de Privilégios:** Realizar auditorias regulares para revisar e ajustar os privilégios dos usuários, garantindo que estejam alinhados com suas responsabilidades atuais.

**Procedimentos para Concessão de Privilégios:** Estabelecer procedimentos claros para a concessão de privilégios, incluindo aprovações formais e documentação adequada para justificar a necessidade de acesso elevado.

**Monitoramento de Atividades de Usuários com Privilégios Elevados:** Implementar um sistema de monitoramento que registre as atividades de usuários com privilégios elevados, garantindo a detecção rápida de comportamentos suspeitos.

**Controle de Acessos:**

**Autenticação de Dois Fatores (2FA):** Implementar a autenticação de dois fatores para garantir uma camada adicional de segurança no acesso a sistemas críticos.

Registros de Acesso: Manter registros detalhados de todos os acessos aos sistemas, incluindo informações como data, hora, usuário e ação realizada.

**Controle Baseado em Funções (RBAC):** Utilizar o modelo de Controle Baseado em Funções para atribuir acessos com base nas responsabilidades e funções específicas de cada colaborador.

**Restrição de Acesso Físico:** Garantir que o acesso físico a áreas críticas, servidores e equipamentos de tecnologia da informação seja restrito apenas a pessoal autorizado.

**Política de Troca de Senhas Regular:** Implementar uma política que exija a troca regular de senhas para garantir a segurança contínua.

**Treinamento de Conscientização:** Fornecer treinamento regular aos colaboradores sobre boas práticas de segurança da informação, incluindo a importância de proteger suas credenciais de acesso.

**Violação da Política e Penalidades Relacionadas a Controle de Privilégios e Acessos:**

No caso de violações nos controles de privilégios e acessos, as penalidades podem incluir:

**Suspensão Temporária de Acesso:** Suspensão temporária dos privilégios de acesso do colaborador infrator.

**Revisão Disciplinar:** Uma revisão disciplinar, que pode resultar em medidas mais severas, dependendo da gravidade da violação.

**Rescisão do Contrato de Trabalho:** Em casos graves e recorrentes, a rescisão do contrato de trabalho pode ser considerada.