POLÍTICA
SEGURANÇA DA INFORMAÇÃO

FUNDAÇÃO DE APOIO AO HOSPITAL DAS CLÍNICAS DA UFG

OBJETIVO

Orientar e estabelecer diretrizes corporativas da sede e das unidades hospitalares da FUNDAHC para a proteção dos ativos de informação, atendendo a ISO/IEC 27001 e a Lei Geral de Proteção de Dados (LGPD).

DIRETRIZES

ABRANGÊNCIA

Aos colaboradores da FUNDAHC, sede e unidades de saúde geridas pela mesma, terceiros internos e externos, todos devendo seguir as orientações e diretrizes para as suas atividades.

A PSI é um complemento destes documentos e aborda, com maior extensão, as questões envolvidas em segurança da informação.

O setor de saúde possui obrigatoriedade legal de manter a confidencialidade (sigilo e proteção) das informações, principalmente, as informações a respeito de seus clientes.

A PSI deve ser lida, compreendida e respeitada por todos os colaboradores (CLT), estagiários, residentes e menores aprendizes que exerçam atividades de gestão ou de prestação de serviços (diretores, gestores, membros de comissões e auditores).

Os terceiros, prestadores de serviço/ fornecedores e parceiros que tenham acesso direto ao ambiente ou participem dos processos da FUNDAHC, também devem ler a PSI e respeitar os controles estabelecidos.

PRINCÍPIOS, REGRAS E PROCEDIMENTOS

Sobre a Segurança da Informação:

Para garantir a Segurança da Informação, suas atividades são baseadas nos seguintes pilares:

Confidencialidade: Garantia de que a informação somente estará acessível para as pessoas autorizadas.

Integridade: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não.

Disponibilidade: Garantia de que a informação estará disponível sempre que for solicitada.

INFORMAÇÕES

Toda informação criada, armazenada, utilizada, copiada, compartilhada e/ ou descartada, são de propriedade da Fundahc/SMS/UFG, não podendo serem utilizadas para motivos pessoais.

É expressamente proibido a divulgação de dados de pacientes, sem o seu consentimento.

Os usuários devem manter a confidencialidade de todas as informações às quais tiverem acesso, mesmo após o encerramento do contrato de trabalho.

SENHA E CERTIFICADO DIGITAL

Nas unidades onde tiver a autenticação nos sistemas baseados em senha ou certificado digital, cada colaborador, parceiro ou prestador de serviço que precisar de acesso, terá seu próprio usuário e senha ou certificado digital.

SENHA

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:

a) A senha é de total responsabilidade do colaborador, sendo expressamente proibido sua divulgação ou empréstimo, devendo ser imediatamente informada ao setor de tecnologia da informação e alterada no caso de suspeita divulgação.

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

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

d) As senhas deverão seguir os seguintes pré-requisitos:

i. Tamanho mínimo de oito caracteres;

ii. Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letra maiúsculas, letra minúsculas, números e caracteres especiais;

iii. Não devem ser baseadas em informações pessoais de fácil dedução (próprio nome, data de nascimento, número do telefone celular, etc).

e) O acesso deverá ser imediatamente cancelado nas seguintes situações:

i. Desligamento do colaborador;

ii. Quando, por qualquer razão, cessar a necessidade do usuário ao sistema ou informação.

f) Para os cancelamentos acima mencionados, o Serviço de Pessoal ficará responsável por informar prontamente o setor de T.I. acerca dos desligamentos e mudanças de função dos colaboradores.

CERTIFICADO DIGITAL

Os certificados digitais, são atualizados anualmente, sendo exigido o modelo em nuvem do tipo A3.

E-MAIL

Todos os setores da sede da FUNDAHC e das unidades, devem possuir e-mail corporativo.

O e-mail é uma as principais formas de comunicação. No entanto, é uma das principiais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

a) o e-mail corporativo é destinado a fins profissionais, relativos às atividades dos colaboradores;

b) É proibido enviar, com o endereço corporativo, mensagens com anúncios particulares, propagandas, vídeos, imagens, musicas, mensagens do tipo “corrente”, campanhas e promoções;

c) É proibido abrir arquivos desconhecidos. Analisar sempre a origens antes de qualquer ação;

d) É proibido enviar e-mails com código executável em anexo (.exe, .cmd, .pif, .js, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer extensão que represente risco a segurança da Informação;

e) O uso do e-mail pessoal é aceitável, se usado com moderação, em caso de extrema necessidade e quando:

i. Não infringir as normas estabelecidas;

ii. Não interferir, negativamente, nas atividades profissionais individuais ou de outros colaboradores;

f) O e-mail corporativo será criado sempre seguindo um padrão:

i. Nome do setor;

ii. Em caso de supervisão, coordenação, encarregado e diretorias, o e-mail terá uma identificação do cargo em seguida com o nome do setor.

INTERNET

Alguns conteúdos da internet estão bloqueados (Pornografia, jogos, bate-papo e redes sociais, streaming (deezer, spotify, etc.), mas os colaboradores devem ficar atentos para não navegar em sites com conteúdo inadequado ao ambiente de trabalho.

Proibido uso de ferramentas P2P (uTorrent, Kazza, Orbit).

DESKTOP

O colaborador deve cuidar da sua estação de trabalho. Sempre que for sair da frente do computador, lembre-se de bloquear (Tecla de Atalho - bandeira do Windows). CTRL+ALT+DEL não bloqueia a tela.

Certifique que o antivírus esteja atualizado. Esse processo é feito por tarefas automatizadas, mas caso não tenha ocorrido, deve abrir uma Ordem de Serviço para corrigir essa situação.

PROIBIDO

- Instalar software, sem autorização de colaboradores da T.I.

- Guardar filmes, MP3 ou softwares no computador.

- Armazenar documentos relacionados ao estabelecimento localmente, devem ser salvos nas pastas mapeadas do servidor, para ser feitos os devidos backups.

-Personalizar o equipamento com adesivos, fotos, riscos, raspar, retirar a etiqueta de patrimônio.

-Alterar o papel de parede.

A equipe de T.I. deve fazer manutenção preventiva dos computadores anualmente, cumprindo um cronograma anual que deve ser entregue no setor de qualidade.

Não é permitido o uso de computadores para assuntos particulares ou externo, fora do contexto da Fundahc.

SOFTWARE

Para instalação ou aquisição de software, o setor deve enviar uma solicitação por O.S. a T.I. para verificação de licenças e sua necessidade.

Softwares, devem possuir base de homologação e produção. Antes de qualquer atualização é necessário testar a versão em base de homologação, para depois atualizar a base de produção.

Os softwares instalados nos computadores deverão sempre estar atualizados, inclusive o próprio sistema operacional.

PENDRIVE

Só é permitido o uso devidamente autorizado pela Diretoria e acompanhado por um profissional de T.I.

REDES SOCIAIS

Existe uma área de comunicação da Fundahc, o qual é responsável por administrar os perfis das unidades administradas pela Fundação. Somente essa área está autorizada a postar informações em nome da Fundahc e das unidades geridas por ela, mediante a consulta junto a Diretoria. Conforme Política de Comunicação.

BACKUP

As cópias de segurança são geradas, referente aos principais arquivos dos estabelecimentos.

Essas cópias são geradas em HD e em servidor exclusivo para esta tarefa.

Os backups são feitos dos documentos do usuário e pastas da rede onde o usuário compartilha arquivos.

Cada estabelecimento tem suas particularidades de backups, de acordo os procedimentos estabelecidos.

O USO DE EQUIPAMENTOS PARTICULARES

O objetivo é minimizar a infecção da rede interna com dispositivos particulares sem controle da equipe de T.I.

a. É vedado o acesso de dispositivo particular (notebook, celulares, tablets e equipamentos afins), na rede cabeada e também na rede Wireless interna, sendo possível, somente, na rede de visitante, se houver.

IMPRESSORAS

Todas as impressões e cópias são monitoradas pela equipe de T.I., no que tange a quantidade de cópias e conteúdo;

O uso de impressora deve seguir as seguintes regras:

a. É proibido a impressão e cópia de documentos de cunho pessoal;

b. A manutenção e configuração das impressoras só podem ser realizadas pela equipe de T.I. da unidade.

ACESSO FÍSICO

Os acessos das unidades são controlados por meio de catracas, com sistema de biometria e/ ou cartão magnético e os ambientes monitorados. As salas de CPD ficam trancadas e a chave com um Responsável da T.I.

ACESSO AO DATACENTER

Os servidores que armazenam os serviços de T.I. da unidade estão localizados em ambiente protegido, sendo totalmente vedado o acesso de pessoas não autorizadas.

Caso haja necessidade de acesso não emergencial, o requisitante deverá solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação do acesso.

O Datacenter deverá ser mantido limpo e organizado.

INTEGRIDADE DA POLÍTICA INTERNA

Periodicamente, os setores serão auditados e os colaboradores devem estar atentos as normas internas.

Setores críticos poderá ser auditado em curto espaço de tempo.

VIOLAÇÃO DA POLÍTICA E PENALIDADES

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

I. Advertência verbal: O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação e será recomendado à leitura desta Norma;

II. Advertência Formal: A primeira notificação será enviada ao colaborador informando o descumprimento da normal, com a indicação precisa da violação cometida; A segunda notificação será encaminhada para a chefia imediata do infrator para que tome as devidas providências.

RECOMENDAÇÕES GERAIS

- Qualquer anomalia nas máquinas ou rede, suspeite e acione a equipe técnica para avaliação, através do sistema de chamado (O.S.).

- Não repasse senha para ninguém, nem deixe anotada em local de fácil acesso próximo à estação de trabalho.

- Não movimente computadores ou troque de tomada sem autorização da equipe técnica.

- As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas à Gerencia de T.I para avaliação e decisão.