INTRODUÇÃO

A Tecnologia da Informação (TI) está cada dia mais presente nas empresas, mudando radicalmente os hábitos e as maneiras de comunicação. É de vital importância a definição de normas de segurança que visem disciplinar o uso da tecnologia da informação. O Complexo Hospitalar Zona Norte (CHZN), baseado na norma NBR ISO/IEC 27.002, definiu sua Política de Segurança da Informação (PSI).

1. OBJETIVO

A Política de Segurança da Informação do INDSH tem como objetivo estabelecer diretrizes para promover a proteção da informação produzida, recebida, utilizada, processada, armazenada e descartada pela Instituição, tanto em seus processos administrativos quanto naqueles relacionados à assistência ao paciente e aos projetos de pesquisas, independentemente de sua forma, sejam elas utilizadas interna ou externamente, com vistas a reforçar o compromisso da Instituição com suas partes relacionadas com relação à segurança das informações por ela manipuladas, e fomentar a cultura de segurança da informação, em linha com a regulamentação nacional e boas práticas internacionais.

2 APLICAÇÃO

Esta Política se aplica a todos os profissionais do INDSH que, direta ou indiretamente, tenham acesso a informações e/ou utilizem recursos tecnológicos da Instituição para a execução de suas atividades profissionais. Esta Política abrange todas as unidades do INDSH, próprias e de contratos de gestão.

3. DEFINIÇÕES E SIGLAS

POL – Política;
CHZN - Complexo Hospitalar Zona Norte
PSI - Política de Segurança da Informação;
TI – Tecnologia da Informação
CCO - Centro de Controle de Operações
VPN: Virtual Private network (Rede privada virtual)

4. RESPONSABILIDADES

Todos os Colaboradores usuários da Infraestrutura de TI, profissionais autônomos, temporários ou de empresas prestadoras de serviço que obtiverem a aprovação por escrito do responsável hierárquico e da gestão de liberações da área de TI para prescrição de senhas de acesso aos recursos computacionais e informáticos do Complexo Hospitalar Zona Norte.
O Complexo Hospitalar Zona Norte (CHZN) entende que o sistema de segurança da informação somente será eficaz com o comprometimento de todos!

4.1 DA ÁREA DE TI

O nosso Departamento de Tecnologia CHZN sempre atua no primeiro atendimento, que é realizado após o usuário abrir o chamado por meio do sistema TIFLUX, em seguida é realizado verificação técnica, com isso é possível certificar se existe algum chamado que necessite ser direcionado as empresas parceiras, entre elas: FLEX SOLUTION, KONEC, COBREL, ENGENHARIA CLÍNICA e ADVEN.

4.2 SEGUE AS ATIVIDADES DESENVOLVIDAS POR CADA FORNECEDOR:

4.2.1 TI - CHZN/ INDSH

- *Criação/ Bloqueio usuário no sistema DGS BRASIL;*
- *Auditoria de usuário no sistema PIXEON;*
- *Instalação de softwares;*
- *Correções de falhas na execução de softwares;*
- *Instalação de drivers de impressoras;*
- *Troca de toner;*
- *Criação de pasta na rede interna;*
- *Suporte Remoto;*
- *Suporte in loco;*
- *Capacitação de usuário;*
- *Criação e configuração de e-mail coorporativo;*
- *Criação de assinatura de e-mail corporativo;*
- *Suporte nos relógios de ponto;*
- *Instalação/ configuração/ Correção de erro no Painel de chamado;*
- *Instalação/ configuração/ Correção de erro no totem (gerenciador de senhas para paciente);*
- *Garantir, assim que solicitado, o bloqueio de acesso de usuários por motivo de desligamento da empresa;*
- *Propor metodologias, sistemas e processos específicos que visem aumentar a segurança da informação;*
- *Promover a conscientização dos colaboradores em relação a relevância da segurança da informação;*
- *Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;*
- *Buscar alinhamento com as diretrizes corporativas da empresa;*
- *Instalar sistemas de proteção, preventivos e detectáveis para garantir a segurança das informações e dos perímetros de acesso;*
- *Monitoramento de latência da rede;*

- *Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente ou superior.*

4.2.2 TI - KONEC

- *Gestão da rede;*
- *Gerenciamento de Firewall;*
- *Gerenciamento de Servidores (VM, AD, DHCP, DNS e VPN);*
- *Gerenciamento de ativos de rede (SWITCH, ROTEADOR e AP);*
- *CFTV;*
- *Sistema de controle de acesso;*
- *Manutenção de impressoras e computadores;*
- *Antivírus;*
- *Fornecimento de Hardwares e periféricos;*
- *Descarte e resíduos de impressoras e hardware periféricos;*
- *Gerenciamento de PABX;*
- *Formatação de computadores;*
- *Remanejamento de computadores.*

4.2.3 TI – FLEX SOLUTION

- *Criação de relatórios no sistema PIXEON;*
- *Criação de documentos no sistema PIXEON;*
- *Criação de formulários no sistema PIXEON;*
- *Atualização do sistema PIXEON;*
- *Gerenciamento do Servidor de aplicação e de dados do sistema PIXEON;*
- *Capacitação de usuários no sistema PIXEON;*
- *Gerenciamento de BI no sistema PIXEON;*
- *Correções de falhas no sistema PIXEON;*
- *Gerenciamento das integrações dos exames laboratoriais;*
- *Gerenciamento das integrações de imagem pelo aplicativo PACS;*
- *Atendimento N2.*

4.2.4 ADVEN

- *Fornecimento de impressoras;*
- *Fornecimento de toner e kit de imagem;*
- *Substituição de kit de imagem;*
- *Remanejamento de impressoras;*

- *Manutenção em impressora;*
- *Administração do servidor de impressão (usuários e relatórios)*
- *Configurações avançadas no scanner.*

4.2.5 COBREL

- *Instalação de rede lógica;*
- *Instalação Elétrica estabilizada (Nobreak);*
- *Instalação de rede telefônica.*
- *Fornecimento de equipamento audiovisual;*
- *Instalação de equipamento audiovisual;*
- *Manutenção em rede lógica, elétrica e telefônica.*

4.2.6 ENGENHARIA CLÍNICA

- *Instalação e configuração de software de diagnósticos.*

4.2.7 PROFISSIONAIS DO INDSH:

1. *Conhecer e cumprir todas as regras definidas nesta Política;*
2. *Adotar a conduta e todos os procedimentos necessários para proteger as Informações da Instituição;*
3. *Abrir chamado para o setor de Tecnologia através do link: https://chzn.org.br/chamado, através da nossa intranet: https://chzn.org.br/intranet ou utilizando o QRCODE disponibilizado na área de trabalho do computador;*
4. *Evitar discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, entre outros), buscando sempre fazê-lo em ambientes adequados e somente com as pessoas que realmente precisam ser envolvidas;*
5. *Utilizar as Informações e os Recursos Tecnológicos da Instituição exclusivamente para os objetivos da Instituição e para o cumprimento de suas funções, sendo vedado o uso para fins pessoais ou de terceiros;*
6. *Solicitar esclarecimentos à Instituição para qualquer dúvida que possa vir a ter quanto ao disposto nesta Política, para que possa cumpri-la, não podendo, em nenhuma hipótese, alegar desconhecimento;*
7. *Relatar para a área de Segurança da Informação eventuais Incidentes de Segurança da Informação ou suspeitas ou violações desta Política das quais venha a tomar conhecimento, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.;*
8. *Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;*
9. *Responder pelo uso exclusivo e não compartilhamento de suas senhas de acesso;*

10. *Ativar suas senhas de proteção para correio eletrônico, sistema operacional e sistemas internos sob orientação do Gestor de Liberações da área de TI;*
11. *Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;*
12. *Assegurar que as informações e dados de propriedade do CHZN não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico;*
13. *Relatar para o seu responsável hierárquico e para o setor de TI o surgimento da necessidade de um novo software para suas atividades;*
14. *Responder pelo prejuízo ou dano que vier a provocar ao CHZN ou a terceiros em decorrência da não obediência as diretrizes e normas aqui referidas.*

5. DOS RESPONSÁVEIS HIERÁRQUICOS:

a) Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão;

b) Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria a responsabilidade do cumprimento da PSI;

c) Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberações da área de TI;

d) Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI;

e) Educar os usuários sobre os princípios e procedimentos de segurança da informação;

f) Notificar imediatamente o gestor de liberações da área de TI, quaisquer vulnerabilidades e ameaças à quebra de segurança;

g) Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;

h) Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor de liberações da área de TI;

i) Obter aprovação técnica do gestor de liberações da área de TI antes de solicitar a compra de hardware, software ou serviços de informática;

j) Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

6. DESCRIÇÃO DA POLÍTICA

6.1 PRINCÍPIOS

A informação produzida ou recebida como resultado de sua atividade profissional pertence ao Complexo Hospitalar Zona Norte (CHZN).

Divulgar informações confidenciais ou estratégicas é crime previsto na lei de propriedade intelectual, industrial (Lei nº 9279/96) e Lei de direitos autorais (Lei nº 9610/98).

A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança.

6.2 ADMISSÃO E DEMISSÃO DE EMPREGADOS

Novos Colaboradores, sendo eles, contratados pelo INDSH ou Terceirizados, antes de iniciar qualquer atividade no seu setor, primeiramente deverão comparecer ao Departamento de Tecnologia CHZN, com a finalidade de criar o usuário de acesso ao computador, e outros acessos relacionados a função, capacitação para abertura de chamado, e por fim, assinar o TERMO DE COMPROMISSO PARA USUÁRIOS DE ATIVOS DE TI, CONFIDENCIALIDADE E SIGILO (FO.CHZN.TI.699).

O setor Recursos Humanos e Departamento Pessoal deverão informar a Tecnologia da Informação - TI:

1. *Toda e qualquer movimentação de temporários, estagiários, admissão e demissão de empregados, para que os mesmos possam ser cadastrados ou excluídos no sistema da instituição;*
2. *Comunicar sobre as rotinas a que os mesmos terão direito de acesso;*
3. *Informar os prazos dos contratos de prestação de serviço, estágio, bem como a demissão/desligamento de empregado, para que na data do encerramento das atividades seja cancelado o acesso do usuário ao sistema.*
4. *Todo ativo (informação) produzido pelo mesmo será mantido pelo INDSH garantindo o reconhecimento e o esclarecimento da propriedade do acervo para a instituição.*

6.3 TRANSFERÊNCIA DE EMPREGADOS / TEMPORÁRIOS / ESTAGIÁRIOS

Quando da transferência, mudança de responsabilidades, de cargo ou atribuições, faz-se necessária a comunicação do Núcleo de Recursos Humanos ao Setor de Tecnologia da Informação para adequação imediata dos direitos de acesso ao sistema informatizado do CHZN.

6.4 EMPREGADOS AFASTADOS

Empregados afastados, por motivo de doença, acidente de trabalho e aposentadoria por invalidez terão seus acessos bloqueados temporariamente nos serviços de e-mails, intranet e softwares, pelo período do seu afastamento.

6.5 IDENTIFICAÇÃO - LOGIN E SENHA:

1. *Os sistemas de Login e senha protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra, e previsto no art. 307 do Código Penal Brasileiro;*
2. *Se existir Login de uso compartilhado por mais de um colaborador, a responsabilidade será dos usuários que dele se utilizarem. Sendo identificada solicitação do gestor para uso compartilhado, este deverá ser responsabilizado;*

3. *Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo);*
4. *É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados;*
5. *As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.). Não devem ser baseadas em informações pessoais, como próprio nome ou de familiares, data de nascimento, endereço, placa de veículo, nome da empresa e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras;*
6. *Os usuários devem proceder a troca de senha caso suspeitem de quebra por terceiros;*
7. *Os logins e senhas devem ser imediatamente bloqueados quando se tornarem desnecessários;*
8. *Tentativa de violação e burla de senhas de acesso, criptografia ou identificação biométrica, se identificada, será alvo de medida disciplinar;*
9. *Os acessos externos à rede de informações do CHZN, fora do expediente de trabalho, serão bloqueados, atendendo a Lei 12.551, trabalho remoto (home office) que altera o Art. 6° da CLT, exceto para casos de emergência relacionados aos serviços de TI.*
10. *Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, por ocasião do desligamento de qualquer colaborador, a Equipe de TI deverá ser comunicada via "abertura de chamado" para Providenciar*
11. *o imediato cancelamento de todas as suas senhas de acesso a equipamentos e sistemas corporativos, bem como de seu e-mail, sendo esse comunicado previamente pela gerência responsável pelo colaborador desligado ou transferido de área.*
12. *Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente através do Gestor para abertura de chamado perante o portal de serviço https://chzn.org.br/intranet/*

6.6 ACESSO A REDE COORPORATIVA E AO BANCO DE DADOS

1. *Todo usuário para acessar os dados armazenados nos servidores do CHZN, deverá possuir um login e senha previamente cadastrados pela Tecnologia da Informação;*
2. *Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação desta Norma;*
3. *Quando for constatada a necessidade de acesso à rede por terceiros, o mesmo deverá solicitar autorização ao Responsável do setor. O acesso deverá ser bloqueado tão logo este tenha terminado o seu trabalho, e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo profissional da Tecnologia da Informação;*

4. *Documentos imprescindíveis para as atividades dos empregados e colaboradores deverão ser armazenados nos Servidores da Rede, tais arquivos, se gravados apenas nas máquinas locais não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;*
5. *Arquivos pessoais e/ou não pertinentes às atividades do CHZN, tais como fotos, músicas, vídeos, etc. não deverão ser copiados/movidos para os "drives" de rede. Caso identificada à existência desses arquivos, eles poderão ser excluídos definitivamente sem prévia comunicação ao usuário;*
6. *O gerenciamento do (s) banco (s) de dados é de responsabilidade exclusiva da Tecnologia da Informação, assim como a manutenção, alteração e atualização de equipamentos e programas.*

6.7 RECURSOS COMPUTACIONAIS:

a) *Os recursos de TI alocados pelo CHZN aos seus usuários são destinados exclusivamente às atividades relacionadas ao trabalho;*
b) *Quando o colaborador utilizar dispositivos de sua propriedade como ferramenta de trabalho no CHZN, seu uso será disciplinado por esta PSI;*
c) *É proibida a intervenção do usuário para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, bem como a transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros (pirataria);*
d) *Todo computador e demais equipamentos em desuso, deverá ser encaminhado a área de TI para a remoção das informações, descarte ou reutilização;*
e) *Não é permitido aos colaboradores tirar fotos, gravar, filmar, publicar e / ou compartilhar imagens dos ambientes internos da Unidade que possam: Comprometer a segurança dos demais colaboradores, comprometer o sigilo das informações, impactar negativamente a imagem da Unidade, outros colaboradores, clientes, parceiros e/ou visitantes.*

7. CLASSIFICAÇÃO DE CRITICIDADE DE INFORMAÇÕES

As informações utilizadas no hospital sustentam o planejamento e aperfeiçoamento no processo decisório de atendimento, todas as atividades estão relacionadas com uso das informações. É dever da TI garantir o bom e constante funcionamento dos serviços ao hospital, no qual são atendidos conforme prioridade.

7.1 PRIORIDADES:

A classificação de prioridade consiste na informação do usuário para o atendimento conforme sua necessidade, acarretando três tipos de prioridade:

***a) PRIORIDADE BAIXA:** áreas não críticas, são considerados atendimentos com a informação descrita de complexidade baixa;*

- *Tempo máximo para atendimento: Em até 12 horas corridas.*

***b) PRIORIDADE NORMAL**: são solicitações de atendimentos com informações de complexidade média em que interfere indiretamente ao paciente;*

- *Tempo máximo para atendimento: Em até 6 horas corridas.*

***c) PRIORIDADE ALTA:** Demanda de informações com alto sigilo e de tramite emergencial que possam interferir diretamente aos processos de rotina normal do hospital. O atendimento deverá ser imediato para as áreas consideradas críticas, nesse caso, onde existe atendimento direto ao paciente, e que não dispõem de outros equipamentos que possam ser utilizados em uma falha na infraestrutura de TI, fato que pode impactar diretamente no trabalho.*

- *Tempo máximo para atendimento: Em até 2 horas corridas.*

8. TELA LIMPA E MESA LIMPA

Deve ser seguido o princípio estabelecido na Norma ABNT NBR/ISO/IEC 27001 da Mesa limpa / Tela limpa. Este princípio tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente. A adoção de uma política de "mesas limpas" para os papéis e mídias de armazenamento removível e, igualmente, uma política de "telas limpas", contra, por exemplo, o perigo de ter um usuário já autenticado / registrado, porém ausente e com sua sessão de trabalho aberta. A política de Mesa Limpa / Tela Limpa busca resguardar o CHZN, bem como o próprio usuário contra o acesso não autorizado a informações como, por exemplo, terceiros observando dados expostos em mesas ou tela, entre outros:

a) *Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa (mesa limpa);*
b) *Informações restritas ou confidenciais devem ser trancadas em local separado (idealmente em um arquivo, armário ou gaveteiro) quando não necessárias, especialmente quando o ambiente ficar vazio;*
c) *Computadores e notebooks não devem ser deixados autenticados / registrados quando não houver um colaborador (operador) junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso (tela limpa);*
d) *Informações restritas ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;*
e) *Não guardar pastas com documentos pessoais/sensíveis em prateleira de fácil acesso;*
f) *Não anotar informações sensíveis em quadros brancos;*
g) *Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas desfragmentadoras;*
h) *Manter os pertences pessoais em gavetas ou armários trancados;*
i) *Nunca deixar crachá de identificação ou chaves em qualquer lugar; mantenha-as junto a você;*
j) *Notificar o pessoal da segurança imediatamente se seu crachá ou chaves sumirem;*
k) *Nunca escrever senhas em lembretes e nem tente esconde-las no local de trabalho;*

l) *Papéis, livros ou qualquer informação restrita ou confidencial não devem ser deixados na mesa;*

m) *Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar computador.*

9. DESCARTE DE MÍDIAS

1. *Mídias contendo informações referentes ao CHZN deverão ser destruídas antes de seu descarte ou guardadas em local seguro;*
2. *CDs, DVDs e documentos em papel deverão passar pelo triturador antes de serem encaminhadas ao lixo, HDs deverão ser encaminhados a TI para a destruição da informação antes do descarte ou reutilização;*
3. *Caso tenha dúvida de como realizar o descarte entrar em contato com o Departamento de Tecnologia.*

10. IMPRESSORAS E COPIADORAS

Os Colaboradores estão cientes de que todo e qualquer uso dos equipamentos, como copiadoras e impressoras, deve ser feito exclusivamente no âmbito das suas atividades profissionais, sendo vedado o uso para fins pessoais. Deve-se evitar imprimir documentos contendo Informações Secretas e, para todos os tipos de informação, os documentos impressos ou copiados devem ser retirados imediatamente dos equipamentos.

10.1. FINALIDADE E USO

a) *O serviço de Impressão destina-se exclusivamente a atividades de cunho institucional;*

b) *A sustentabilidade ambiental é elemento chave na utilização do serviço – a impressão de documentos deve ser evitada sempre que possível;*

c) *Deve-se sempre usar impressão em face dupla;*

d) *Deve-se, se possível, imprimir em modo econômico;*

e) *Deve-se buscar a tramitação de processos administrativos sempre na forma eletrônica,*

f) *fazendo uso da impressão apenas nos casos onde se requer assinatura ou carimbos impressos, não sendo possível usar assinatura digital;*

g) *As impressoras são alocadas nos centros de custo conforme demandas apresentadas;*

h) *Não imprimir documentos apenas para lê-los. Leia-os na tela do computador, se possível;*

i) *É de responsabilidade dos centros de custo da alocação racional deste recurso, reduzindo custos pelo compartilhamento de equipamentos;*

j) *Toda impressão realizada através do serviço deve ser associada a um único usuário;*

k) *Informações sobre o número de páginas e título dos documentos, assim como data e hora da impressão, assim como o usuário responsável, são registradas e mantidas por tempo indeterminado;*

l) *O responsável pelo centro de custo poderá implementar uma política de quotas de*

m) *Impressão;*

n) *Os custos associados ao serviço serão repassados aos respectivos centros de custos.*

10.2. INFRAESTRUTURA DO SERVIÇO DE IMPRESSÃO

a) *O Hospital Delphina Aziz recebe equipamentos que são contratados na forma de serviço e incluem manutenção de defeitos, fornecimento de toner e outros suprimentos, descarte e reciclagem de partes e peças substituídas. Somente o papel deve ser fornecido pela unidade usuária do serviço;*

b) *São fornecidos diferentes modelos de impressora com custos e capacidades diferenciados;*

c) *Cada impressora tem um custo fixo por página, conforme seu modelo;*

d) *Poderá existir uma franquia de impressão, que estabelece o quantitativo mínimo de*

e) *impressões para viabilizar o planejamento financeiro dos serviços.*

f) *Poderão ser implementados mecanismos para redução de impressão como limite de páginas de um documento, redirecionamento de documentos grandes para impressoras com custo menor, limite de cópias de documentos, tempo mínimo entre impressões, tempo de descarte e obrigatoriedade da autorização presencial para início da impressão.*

11. CLASSIFICAÇÃO DA INFORMAÇÃO

- *O gestor de cada área deve estabelecer os critérios relativos ao nível de confidencialidade da informação gerada por sua área em: Pública, Confidencial ou Interna.*

12. SEGURANÇA CIBERNÉTICA

a) *A TI disponibiliza software corporativo de antivírus instalado para todos os usuários;*

b) *O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor;*

c) *As checagens periódicas do disco rígido, HD, da estação de trabalho estão programadas para execução periódica automática, conforme definições da área de TI no aplicativo servidor.*

d) *Todos os dados digitais são armazenados em um servidor físico, que está instalado no CCO – Centro de Comando Operacional, que é monitorado 24hrs, por câmeras de segurança, agente de segurança, virtualmente por segurança de firewall e monitoramento de rede. É realizado diariamente backup das informações contidas no servidor interno para um servidor em nuvem de forma criptografada.*

e) *Para maior segurança, todos os ativos(computadores) recebem periodicamente atualização (PATCH) de segurança pelo fornecedor do sistema operacional, mantendo assim o sistema mais seguro e estável.*

f) *Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante abertura de chamado no portal de serviço https://chzn.org.br/intranet/. Para o caso de o antivírus detectar "comportamento suspeito" proveniente de algum equipamento da Unidade, o mesmo poderá ser isolado da rede pelo time de Operações de TI sem aviso prévio ao usuário.*

13. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Cabem, primariamente, à área de Segurança da Informação as ações de prevenção de Incidentes de Segurança da Informação, atuando conforme normativos específicos. Porém, é responsabilidade de todo e cada Profissional do INDSH atentar para qualquer evento suspeito e comunicar imediatamente ao gestor imediato, para as devidas providências.

14. SALVAGUARDA DE ARQUIVOS

1. *Compete ao gestor de continuidade da área TI criar e manter cópias de segurança (backups) apenas dos dados armazenados nos servidores de rede;*
2. *Todos os dados confidencias deve ser armazenado em sistemas seguros, com acesso restrito baseado no princípio do "mínimo privilégio";*
3. *Os usuários devem manter obrigatoriamente os documentos, planilhas, e-mails, apresentações, desenhos e outros dados críticos do CHZN, nas pastas departamentais dos servidores de rede;*
4. *É de responsabilidade exclusiva do usuário a cópia de segurança (backup) e a guarda dos dados gravados da sua estação local de trabalho;*
5. *O CHZN realiza diariamente backup, sendo eles, nos servidores locais e em nuvem;*
6. *Os principais backups realizados diariamente, são eles, banco de dados do sistema prontuário eletrônico, sistema PACS, arquivos setoriais e outros;*
7. *Toda solicitação de restauração de backup, deve ser solicitado juntamente pelo Gestor da área através de e-mail enviado para o departamento de tecnologia, pelo endereço ti.chzn@indsh.org.br*

14.1. TODAS AS AÇÕES RELACIONADAS À SEGURANÇA DA INFORMAÇÃO DEVERÃO SER NORTEADAS PELOS SEGUINTES PRINCÍPIOS:

I. ***Propriedade:*** *A Informação, em qualquer forma ou suporte que se apresente (verbal, escrita, físico ou digital), e os Recursos Tecnológicos disponibilizados aos Profissionais do INDSH*

são de propriedade da instituição ou do ente público que o INDSH possui contrato de gestão, tendo natureza exclusiva de ferramentas de trabalho;

II. ***Confidencialidade:*** *A Informação deve ser conhecida somente por pessoas autorizadas, que precisem conhecê-la para o desenvolvimento de suas atividades profissionais e nos limites estritamente necessários ao desempenho de suas respectivas funções, e exclusivamente para o atendimento dos objetivos do negócio da Instituição;*

III. ***Integridade:*** *A Informação deve ser armazenada de forma a garantir a exatidão, atualização e completude de seu conteúdo;*

IV. ***Disponibilidade:*** *A Informação deve estar disponível para o acesso de pessoas autorizadas, quando necessário ao cumprimento das finalidades de uso das Informações na forma definida pelas políticas e diretrizes da Instituição sobre o tema;*

V. ***Monitoramento e Auditoria:*** *Para garantir a segurança das Informações tratadas pela Instituição, o cumprimento de suas políticas internas e da legislação e regulamentação aplicável, o uso da Informação e dos Recursos Tecnológicos da Instituição estão sujeitos a controle e monitoramento constantes, nos termos desta Política. O resultado do controle e monitoramento pode ser utilizado para auditorias e avaliações visando à constatação de violação desta Política e demais códigos, políticas, processos e procedimentos da Instituição, bem como da legislação e regulamentação aplicáveis, inclusive para a defesa dos direitos e interesses da Instituição e para a aplicação de medidas disciplinares e exercício de direitos em processos administrativos e/ou judiciais, conforme o caso;*

VI. ***Garantia da Privacidade e da Proteção dos Dados de Pacientes e de Titulares de Dados Pessoais:*** *A Instituição e os Profissionais do INDSH são responsáveis pela segurança de quaisquer Informações e dados por ele administrados, devendo garantir a confidencialidade, integridade e disponibilidade destas Informações, prevenindo assim Incidentes de Segurança de Informação de qualquer natureza envolvendo o tratamento e a proteção de dados, em especial dados relacionados à saúde de pacientes, considerados Dados Pessoais Sensíveis nos termos da legislação vigente. Da mesma forma, projetos de pesquisa devem garantir a privacidade e a proteção dos dados de pacientes, incluindo, mas não se limitando a, dados cadastrais, clínicos, biomoleculares e laudos;*

VII. ***Acesso e Guarda de Prontuários:*** *Os prontuários pertencem exclusivamente aos pacientes. À Instituição, como depositária deste documento, cabe o dever de zelar por sua integridade, confidencialidade, disponibilidade e guarda segura, gerenciando-os de forma a atender integralmente os requisitos da legislação vigente. Os prontuários, sejam eles em versão física ou eletrônica, somente deverão ser disponibilizados aos Profissionais do INDSH que necessitarem acessar aquelas informações, para finalidades determinadas e justificadas. Sempre que possível, o acesso deve ser modulado, concedendo ao usuário acesso restrito exclusivamente às Informações necessárias. Os prontuários devem ser guardados (I) de forma segura, resguardando a integridade física dos documentos, e sistematizada,*

possibilitando a localização, armazenamento e recuperação dos documentos; e (II) pelo tempo que determinar a legislação aplicável;

VIII. ***Propriedade Intelectual:*** *A propriedade sobre o conhecimento, processos, informações, dados, produtos, documentos, livros, relatórios, resultados tangíveis e intangíveis, sistemas, ferramentas, plataformas e tecnologias geradas em projetos de pesquisas será regulamentada por padrões institucionais específicos sobre propriedade intelectual, os quais deverão ser integralmente observados por todos os Profissionais do INDSH.*

15. SEGURANÇA FÍSICA

A Segurança da Informação se faz também com o estabelecimento de mecanismos de proteção física. A criação de barreiras físicas que previnam acessos não autorizados, tais como leitores biométricos, portas de acesso com cartões magnéticos, entre outras medidas, devem ser utilizadas na medida em que forem necessárias para a proteção de Informações e dos Recursos Tecnológicos, em especial aquelas registradas em meio físico.

16. ACESSO REMOTO

O acesso remoto consiste na disponibilização aos Profissionais do INDSH de ferramentas de acesso à Informação como medida de apoio para a execução de suas atividades profissionais. São regras gerais para o acesso remoto:

I. O acesso remoto é considerado de caráter excepcional e deve ser autorizado formalmente, por período determinado, conforme políticas institucionais;

II. O acesso remoto somente poderá ser concedido mediante o uso de ferramentas de proteção do ambiente computacional fornecidas pelo INDSH, por meio de ferramentas devidamente homologadas pela Instituição;

III. É proibido franquear acesso remoto a terceiros não autorizados.

17. ARMAZENAMENTO DE ARQUIVOS

a) *Todos os arquivos contidos nos servidores de rede ou nas estações de trabalho dos usuários devem ser exclusivamente de interesse do CHZN.*
b) *É proibida a criação de pastas pessoais nos servidores de rede;*
c) *A criação de pastas departamentais nos servidores de rede deverá refletir a estrutura organizacional do CHZN e ser solicitada pelo responsável hierárquico ao gestor de liberações da área de TI;*
d) *O acesso às pastas departamentais nos servidores de rede, exige autorização do responsável hierárquico e do gestor de liberações para o controle do acesso de cada usuário;*
e) *A partir da implantação desta política, todos os arquivos que não sejam do interesse do CHZN deverão ser excluídos dos equipamentos para evitar problemas futuros com auditorias.*

f) *Todos as pastas setoriais que foram criadas de forma oficial por via solicitação para o Departamento de Tecnologia são protegidas por perdas, seus backups realizados diariamente.*

18. UTILIZAÇÃO DA REDE

1. *O CHZN possui uma rede integrada de computadores com servidores e um microcomputador para cada colaborador alocados na Unidade;*
2. *O acesso à rede do CHZN só poderá ser efetivado após o registro obrigatório de computadores e usuários, de acordo com os sistemas de registro implementados;*
3. *O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso;*
4. *Os colaboradores do CHZN não deverão obter ou disponibilizar material sem a licença adequada através da rede;*
5. *O usuário é responsável pela própria e devida autenticação nos sistemas de disponibilizados pelo CHZN, não podendo fornecer e ou compartilhar seu usuário, senha e ou acessar com outros usuários;*
6. *O usuário está comprometido a utilizar a rede interna do CHZN para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence;*
7. *É vedada a utilização de PROXY e VPN ou similar que permitam o tráfego de informações a redes privadas externas;*
8. *Os usuários devem administrar suas pastas, excluindo arquivos desnecessários tais como:*
   a) *Material sexualmente explícito ou contrário à legislação brasileira não podem ser expostos, armazenados, distribuídos, editados ou gravados, através do uso dos recursos computacionais da rede corporativa da empresa;*
   b) *Gravação de arquivos particulares (músicas, filmes, fotos etc.);*
   c) *Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, sem prévia comunicação;*
   d) *Os sistemas corporativos são os sistemas utilizados na gestão CHZN, os quais buscam trazer maior transparência, conveniência e confiabilidade para as informações, abrangendo todos os segmentos da administração da organização e permitindo o gerenciamento isolado de cada parte e a interligação desta com o todo, produzindo relatórios analíticos, sintéticos e estatísticos, sendo acessados por meio de uma rede interna ou externa;*
   e) *É expressamente proibida a divulgação e ou o compartilhamento indevido das informações contidas nos sistemas corporativos do CHZN.*
   f) *Todos os usuários dos ativos de informação de propriedade do CHZN, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do mesmo, mantendo conduta profissional;*
   g) *O acesso às informações contidas nos sistemas corporativos deve ser efetuado sempre através de identificação segura (login e senha);*

h) Para cada usuário devem ser atribuídas permissões específicas, por módulo e/ou operação;

i) A concessão de acesso às bases de dados para prestadores de serviço e colaboradores deverá sempre seguir o critério do menor privilégio possível.

19. UTILIZAÇÃO DA INTERNET

A internet é o instrumento que deverá ser usado, exclusivamente, para o desempenho das atividades relacionadas ao CHZN. O uso pessoal de ordem eventual poderá ser permitido, desde que não consuma recursos significativos de tempo ou interfira na produtividade pessoal. "Sites" que não contenham informações que agreguem conhecimento profissional e/ou para as atividades do CHZN não devem ser acessados.

O uso da Internet será monitorado pela Tecnologia da Informação, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou. Portanto, o CHZN aplica algumas restrições de acesso à internet para os usuários, abaixo descriminadas:

a) Utilizar a Internet com objetivos ou meios para a prática de atos ilícitos, proibidos pela lei ou pela presente política, lesivos aos direitos e interesses da organização ou de terceiros;

b) Utilizar a Internet com objetivo de danificar, inutilizar, sobrecarregar ou deteriorar os recursos de tecnologia da informação e dados de qualquer tipo, de uso corporativo, pessoal ou de terceiros;

c) É proibido aos usuários de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários;

d) O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações das empresas abrangidas neste procedimento;

e) Acessar a sites de proxy com o objetivo de burlar os mecanismos de segurança existentes;

f) Acessar sites de pornografia, pedofilia, erotismo e correlatos de racismo, de ferramentas para invasão e evasão de sistemas, de compartilhamento de arquivos e de apologia e incitação a crimes e outros contrários à lei. O acesso a esses sites é terminantemente proibido, ainda que os mesmos não estejam bloqueados no sistema de segurança da organização;

g) Não será admitido burlar ou tentar burlar os filtros de conteúdo ou restrições de acesso à internet, sob pena de responsabilização dos envolvidos, que estarão sujeitos às sanções administrativas e penais cabíveis;

h) Os equipamentos fornecidos para o acesso à internet são de propriedade do OPY ou de responsabilidade da mesma através de um contrato de locação de terceiros.

Assim, a organização poderá analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados em disco local, na rede ou internet;

i) *Assim, a organização, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.*

j) *É proibido aos usuários configurar ou alterar as configurações de rede e de acesso à Internet dos computadores, incluindo as seguintes configurações de rede: IP, DNS, WINS, Gateway, Proxy e a instalação ou reconfiguração de clientes Proxy. Em caso de dúvidas, solicitar orientação ao Departamento de Tecnologia;*

k) *Não é permitido enviar (upload), baixar (download) ou manter arquivos de imagens, músicas, vídeo, arquivos executáveis em geral ou quaisquer outros de caráter pessoal;*

l) *É proibido o acesso a sites de redes sociais, dos quais fazem parte: Badoo, Par Perfeito, Linkedin, Instagram, Twiter, Facebook ou assemelhados, com exceção ao Facebook, quando houver necessidade funcional por parte do usuário/setor para divulgação das ações do CHZN;*

m) *Não é permitido o acesso a sites de Internet com conteúdo de jogos, bate-papo, chat, cartoon, relacionamento, rádio e TV em tempo real, hacker ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança;*

n) *É proibida a divulgação de informações confidenciais do CHZN por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensagens ou bate-papo, blogs, microblogs, ou ferramentas semelhantes.*

o) *Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos;*

p) *A internet, via Wi-Fi, deverá ser utilizada para fins corporativo, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades do CHZN;*

q) *O colaborador é responsável pelas atividades realizadas por intermédio de seu login e senha de acesso. Em particular, o usuário deverá observar os termos de licença de uso do material obtido através da internet.*

20. ACESSO A REDE WIRELESS (REDE SEM FIO)

A rede sem fio permitirá que usuários ou visitantes portadores de equipamentos pessoais, dotados da tecnologia sem fio, acessam a internet da Unidade, mediante formalização feita pelo Gestor da área, que deverá ser solicitada a Tecnologia da Informação.

21. SOLICITAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA

Toda solicitação de novos equipamentos de informática deverá ser feita a Tecnologia da Informação, por meio de um MEMORANDO, devidamente datado e assinado pelo responsável pelo Setor.

Define-se como equipamentos de informática quaisquer artigos do tipo hardware utilizados na instituição e gerenciados pela Tecnologia da Informação, como computadores, notebooks, kit multimídia (caixa de som e alto-falantes), câmeras digitais, projetores, cabos específicos e extensões, adaptadores, mouse, teclado, monitores, impressoras, gravadora portátil de CD/DVD, CPU´s, HD externo, etc.

Para saber mais sobre o processo interno consulte o fluxo: FLU.CHZN.274:01 - Aquisição de novas tecnologias.

22. INSTALAÇÕES DE SOFTWARE

O colaborador do CHZN é proibido de instalar todo e qualquer programa não autorizado em seu computador e em qualquer outro dispositivo computacional pertencente à organização, salvo as instalações de programas que contenham prévia autorização da área de TI. Este comando também é aplicado a programas com conteúdo de atualização conhecidos como patches. O usuário é proibido de remover toda e qualquer versão de software obsoleto, mesmo em casos onde exista uma versão atualizada da aplicação utilizada. Caso o usuário necessite instalar ou remover qualquer software, deverá solicitar a área de TI via chamado.

Não é permitida a instalação / uso de softwares ilegais (sem licenciamento), sendo que a área de TI poderá valer-se desta Política para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software). É proibido executar

programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da organização.

23. PRONTUÁRIO ELETRÔNICO

a) *O prontuário do paciente é um dos documentos mais importantes no registro do histórico de atendimento multiprofissional na área de saúde, registrando cada passo deste processo, passando pelos atestados, laudos de exames e prescrições médicas, entre outros itens, além de assegurar a continuidade do tratamento. Trata-se de um documento de propriedade do paciente, que tem total direito de acesso.*

b) *O conjunto de normas que regula este assunto prevê, por exemplo, que é proibida a produção de fotos, fotocópias, digitalização ou cópias digitais em partes do prontuário clínico ou no seu todo, sem a autorização prévia, por escrito, por parte do paciente ou nas demais situações previstas legalmente. Também são proibidas a retirada, a adulteração*

ou a destruição de qualquer documento do prontuário, assim como qualquer comentário verbal ou por meio eletrônico de dados sobre o paciente sem a sua autorização.

c) *A desfiguração ou destruição de documentos de valor permanente considerados de interesse público e social sujeitam o infrator à responsabilidade penal, civil e administrativa, na forma da legislação em vigor;*

d) *O Hospital Hospital Delphina Rinaldi Abdel Aziz se baseia em todas estas normas legais, que vão desde resoluções, regulamentos e recomendações de várias instituições até a Constituição Federal;*

e) *As informações pessoais que contenham históricos de saúde são conceituadas pela LGPD como dados pessoais sensíveis, exigindo especial atenção, uma vez que eventual incidente de segurança com esse tipo de dado pode trazer consequências graves aos direitos e às liberdades dos titulares, garantidos pela Constituição Federal. Por isso, o cuidado na entrega do prontuário médico, a fim de evitar vazamento de informações;*

f) *Todos os profissionais que têm acesso ao prontuário têm o dever de observar e respeitar os direitos fundamentais de liberdade, de intimidade e de privacidade dos pacientes, expressamente previstos no artigo 17 da LGPD, reforçando a previsão expressa da Constituição Federal, artigo 5º;*

g) *Em particular, devem ser previstas formas e estruturas institucionais para, em segurança, dar conhecimento e acesso do prontuário ao paciente ou a terceiros autorizados, conforme deveres previstos no artigo 18 da LGPD.*

h) *Sobre atualização – Toda parada do servidor com a finalidade de atualizar o servidor de banco, servidor de aplicação e upgrade do servidor, será informado com antecedência pelos canais de comunicação interna disponibilizado pelo setor ASCOM.*

24. E-MAIL E MENSAGENS INSTANTÂNEAS

- *É proibido o uso de e-mails, correios eletrônicos ou mensagens instantâneas de forma contrária a lei, a moral, aos bons costumes, à ordem pública ou que infrinjam os direitos a propriedade intelectual ou industrial pertencente a terceiros;*
- *O conteúdo e a utilização de e-mails, correios eletrônicos ou mensagens instantâneas deve ser de caráter exclusivamente profissional;*
- *Os serviços de mensagens instantâneas são permitidos apenas para os usuários autorizados pela hierarquia do CHZN;*
- *O uso de software de e-mail, mensagens instantâneas e correio interno não homologado pela Diretoria de Administração e Custos são de responsabilidade do usuário e podem trazer riscos à segurança da informação além de dificultar o suporte técnico;*
- *Quaisquer comunicados em massa, propagandas, informativos, imagens, etc., deverão ser previamente aprovados pelo gestor de capacidades da área de TI, afim de não serem tratados como Spam ou comprometerem o funcionamento dos sistemas de e-mail;*

- *Mensagens recebidas de origem desconhecida deverão ser pré-visualizadas e eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos.*
- *O uso indevido do e-mail é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado pelos danos causados;*
  - *a) As mensagens trafegadas sob o domínio do CHZN poderão ser auditadas, mediante solicitação, conforme "definição" para "entendimento majoritário dos julgadores" Desta forma é proibida a utilização particular.*
  - *b) Em nenhuma hipótese o CHZN será responsabilizado perante quaisquer usuários ou terceiros pela perda de mensagens e/ou respectivo conteúdo;*
  - *c) O fato de o colaborador responder a um e-mail fora do horário de expediente não configurará hora extra. Para que isto ocorra é necessário que o CHZN exija por e-mail, a realização de uma tarefa fora do horário de trabalho.*

25. UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS CORPORATIVOS

Dispositivos móveis corporativos são equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória.

- *a) É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações de uso interno, restritas ou confidenciais por meio de dispositivos móveis corporativos;*
- *b) O usuário deve utilizar os dispositivos móveis corporativos de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;*
- *c) O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis corporativos, tanto por sua guarda, quanto pelos conteúdos neles instalados;*
- *d) Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel corporativo;*
- *e) Não é permitida a alteração da configuração dos sistemas operacionais dos equipamentos, em especial, os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um colaborador da área de TI;*

f) *O colaborador deverá responsabilizar-se por não utilizar quaisquer programas e/ou aplicativos, inclusive gratuitos, que não tenham sido instalados ou autorizados por um colaborador da área de TI;*

g) *É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo CHZN, notificar imediatamente seu gestor e a área de TI. Também deverá, assim que possível, registrar um Boletim de Ocorrência na Delegacia de Furtos de Roubos (BO);*

h) *O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracteriza a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a organização e/ou a terceiros;*

i) *Em caso de desligamento, o colaborador deve realizar imediata devolução de seus dispositivos móveis à área de TI e assinar o termo de devolução do equipamento.*

26. UTILIZAÇÃO DE MÍDIAS REMOVÍVEIS

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais. Tal vulnerabilidade não pode ser contida com "firewalls" já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa.

Para minimizar os riscos de exposição e perda de dados sensíveis mantidos pela empresa e reduzir os riscos de proliferação de "malwares" nos computadores, a transferência de informações para dispositivos removíveis é bloqueada nos equipamentos da empresa.

27. AUDITORIAS

- *A Direção do CHZN poderá solicitar relatórios de auditoria contendo o nome, mensagens trafegadas, acessos ao sistema e demais informações do usuário;*
- *O processo de auditoria será mediante a solicitação do gestor da área;*
- *Esse processo de auditoria está relacionado ao sistema DGS BRASIL.*

28. CICLO DE VIDA DA INFORMAÇÃO

O INDSH deverá garantir a segurança das suas informações durante todo o ciclo de vida destas, da geração ao descarte, que pode variar a depender do tipo e relevância de cada uma destas informações e da legislação correspondente.

Será considerado tratamento de dados tudo aquilo que a legislação determina, tais colo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Os tratamentos mais comuns nas unidades geridas pelo INDSH são:

I. *Recepção: cadastro dos pacientes.*

II. *Acesso: quando da análise clínica dos pacientes, os profissionais de saúde acessam os dados dos pacientes.*

III. *Arquivamento/armazenamento: guarda do prontuário médico, que pode ser físico (papel) ou lógico (dados).*

IV. *Transferência: quando se transfere os dados dos pacientes para um serviço em nuvem.*

V. *Eliminação: quando e como a informação é descartada.*

29. FORNECEDORES

A área de Segurança da Informação deverá implementar manual, diretrizes, normas e procedimentos específicos para avaliação (due diligence), contratação e monitoramento constante de fornecedores no que tange a seu nível de conformidade com os requisitos de controles técnicos de Segurança da Informação, em conformidade com esta Política, demais normativos da Instituição e as melhores práticas de Segurança da Informação.

30. PLANO DE CONTINGÊNCIA:

- *Um plano de contingência e continuidade do negócio deverá ser implementado e testado anualmente. O objetivo é reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, por meio da combinação de ações de prevenção e recuperação;*
- *Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados, na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução;*
- *Toda falha no processo, seja ela, por conexão de internet, impressora, rede elétrica, rede de dados/ internet, ramal, arquivos em rede, sistema de prontuário eletrônico e equipamentos em geral, será primeiramente verificado se foi uma interrupção geral ou parcial, após análise do Departamento de Tecnologia, seguirá para o plano de contingência ou não.*

O usuário antes de prosseguir com a solicitação do suporte, deverá realizar as ações abaixo:

DESCRIÇÃO	AÇÃO	SOLUÇÃO
Conexão de rede e internet	• Verificação se os cabos estão conectados corretamente; • Verificar se os demais computadores também estão sem acesso; • Realizar reinicialização do computador;	• Realizar abertura de chamado utilizando o QRCODE, ou através da nossa intranet na aba abertura de chamado • acessando o site: chzn.org.br/chamado;

	• Verificar se o monitor ou a "CPU" está em funcionamento(energia); • Identificar no canto inferior o ícone de conexão à internet.	• Ligue nos ramais: 1638/1639/1640
Impressora	• Verificar se a impressora está instalada; • Identificar se o nome da impressora instalada com o nome do seu setor; • Verificar se a impressora está ligada na tomada; • Reiniciar o computador; • Em caso de ligada na tomada, apertar o botão Power (ligar) da impressora; • Verificar no visor da impressora se está com mensagem de troca de toner; • Identificar no visor se está com mensagem de troca de UND. De IMG.	• Realizar abertura de chamado utilizando o QRCODE, ou através da nossa intranet na aba abertura de chamado • acessando o site: chzn.org.br/chamado; • Ligue nos ramais: 1638/1639/1640
Pasta na rede	• Antes de conseguir acessar a pasta da rede, verifique com o seu gestor se você tem permissão; • Reiniciar o computador	• Realizar abertura de chamado utilizando o QRCODE, ou através da nossa intranet na aba abertura de chamado • acessando o site: chzn.org.br/chamado; • Ligue nos ramais: 1638/1639/1640
Sistema de prontuário eletrônico	• Em caso de mensagem de erro reiniciar o computador; • Em casos de erro de erro de login, realizar reset de senha clicando na opção "esqueceu a senha"; • Verificar mensagem de erro e repassar para Suporte; • Criação ou permissão de usuário serão dadas conforme autorização; • Verificar se o perfil está de acordo com a solicitação e acesso no sistema.	• Realizar abertura de chamado utilizando o QRCODE, ou através da nossa intranet na aba abertura de chamado • acessando o site: chzn.org.br/chamado; • Ligue nos ramais: 1638/1639/1640.
Hardware (equipamentos de tecnologia)	• Em caso de monitores, e CPU's validar se a mesmas estão ligadas na tomada; • Sempre verificar se os cabos de energia estão conectados nos equipamentos; • Em caso de mouse e teclado, realizar verificação de usabilidade; • Reiniciar o computador;	• Realizar abertura de chamado utilizando o QRCODE, ou através da nossa intranet na aba abertura de chamado • acessando o site: chzn.org.br/chamado; • Ligue nos ramais: 1638/1639/1640

Energia elétrica	• Interrupção de Energia, Queda constante e tomadas não funcionado;	Ligar para o CCO: 1283 e solicitar apoio técnico.
TELEFONIA	• Primeiramente verificar se o ramal mais próximo está fora, pode ocorrer de ser problema no aparelho telefônico.	Realizar ligação para empresa COBREL através do ramal: 1283.

O Departamento de Tecnologia irá informar os responsáveis em caso do sistema não retorne no prazo de 15 minutos, com objetivo de iniciar o plano de contingência, que é feito através dos documentos no sistema Qualyteam, conforme descrito no Fluxo - FLUX.CHZN.TI.273.
Acesso ao sistema Qualyteam - Através da nossa intranet: https://chzn.org.br/intranet ou através do site: https://indsh.qualyteam.com.br/. O usuário e senha está disponível através de um adesivo fixado no monitor do usuário.
Em caso de falha de acesso a internet, o sistema Qualyteam ficará offline, será necessário utilizar o 2ª plano de contingência, para isso utilize a pasta disponível na rede interna, vá até sua área de trabalho, e clique no ícone com a descrição plano de contingência.
Nossa Assessoria de Comunicação – ASCOM, irá realizar a transmissão da informação através dos meios de comunicações, seja ela por linha de transmissão, intranet e outros.
Nossos planos de contingências implantados e disponíveis são:

- *FLU.CHZN.273:01 - Plano de contingência PIXEON;*
- *IT.CHZN.142:01 - Plano de Contingência TI.*

31. RESPONSABILIDADE INSTITUCIONAL:

A todos os colaboradores:

- *Conhecer e cumprir a presente política;*
- *Assinar TERMO DE COMPROMISSO PARA USUÁRIOS DE ATIVOS DE TI sobre a política declarando ter conhecimento de suas responsabilidades;*
- *Buscar orientação em caso de dúvidas relacionadas à segurança da informação;*
- *Fiscalizar e orientar os parceiros e clientes da organização quanto às diretrizes desta política;*
- *Observar os princípios constantes no Código de Ética;*
- *Comunicar imediatamente o seu Gestor quando do descumprimento ou violação desta política.*

32. DISPOSIÇÕES FINAIS

- *Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do CHZN. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.*

- *O Departamento de Tecnologia exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Profissionais, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.*
- *Todas as práticas que ameacem à segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado ao CHZN, entre outros.*

33. ANEXOS

FO.CHZN.TI.699 - TERMO DE COMPROMISSO PARA USUÁRIOS DE ATIVOS DE TI, CONFIDENCIALIDADE E SIGILO.

34. REFERÊNCIAS BIBLIOGRÁFICAS

1. https://dokumen.pub/abnt-nbr-iso-iec-270022013-tecnologia-da-informaao-tecnicas-de-segurana-codigo-de-pratica-para-controles-de-segurana-da-informaao-abnt-nbr-iso-iec-270022013-2nbsped-9788507046134.html
2. http://micreiros.com/norma-nbr-isoie
3. https://www.youtube.com/watch?v=5_D9byj5y9c
4. http://www.planalto.gov.br/ccivil_03/leis/l9279.html
5. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12551.htm
6. https://www.gov.br/ebserh/pt-br/hospitais-universitarios/regiao-sul/hu-ufsc/comunicacao/noticias/leis-regulam-acesso-ao-prontuario-e-defendem-privacidade-do-paciente
7. Lei Federal nº 8.159 de 08 de janeiro de 1991 (Dispõem sobre a Política Nacional de Arquivos Públicos e Privados).
8. Lei Federal nº 10.406 de 10 de janeiro de 2002 (Institui o Código Civil).
9. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)
10. Decreto nº 4.453, de 27 de dezembro de 2002 (Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal).
11. Decreto n° 9.637, de 26 de dezembro de 2018 (Institui a Política Nacional de Segurança da Informação).
12. Norma ABNT/NBR ISO 27.701/2019.

TERMO DE COMPROMISSO PARA USUÁRIOS DE ATIVOS DE TI, CONFIDENCIALIDADE E SIGILO

(Este termo de compromisso aplica-se a todos os usuários de ativos de tecnologia da informação do CHZN)

Declaro que li e estou de acordo com a ***Política de Segurança da Informação*** *do CHZN e com Recomendações de Usuários, tendo ciência de todo o seu conteúdo. Declaro, ainda, estar ciente de que incidentes contrários à política de segurança resultarão em medidas que poderão chegar inclusive ao meu desligamento do quadro efetivo do CHZN, à quebra de contrato, aos processos judiciais ou a outras medidas pertinentes.*

Comprometo-me a preservar a integridade, a disponibilidade, a confidencialidade e o sigilo de toda e qualquer informação relacionada a paciente, a que tiver conhecimento em razão da prestação laboral no Hospital Delphina Rinaldi Abdel Aziz das informações obtidas durante a vigência do contrato com o CHZN, mesmo após o seu encerramento.

Em sendo prestador de serviço terceirizado comprometo-me igualmente no cumprimento das regras e diretrizes previstas na PSI, bem como do presente Termo.

Reconheço que estou sendo mais uma vez orientado e ora reconheço minha inequívoca ciência sobre minhas obrigações profissionais quanto ao sigilo e confidencialidade das informações dos prontuários, imagens dos pacientes ou qualquer outra forma de identificação do paciente, cuja revelação indevida a terceiros resultará em sanções trabalhistas, criminais e éticas perante os conselhos de classe respectivos e poderá levar ao pagamento ou recomposição de todas as perdas e danos comprovados pela vítima (pacientes/familiares/responsáveis legais) e pelo empregador. É proibido, por exemplo, mas não unicamente:

- *Fotografar ou filmar acompanhantes, pacientes e seus prontuários;*
- *Divulgar informações que identifiquem pacientes, seu quadro de saúde e sobre a assistência médico-hospitalar prestada nesta unidade de saúde por qualquer meio, inclusive mídias sociais e grupos privados de mensagens (Facebook, Instagram, WhatsApp, Telegram e outros);*
- *Compartilhar ou divulgar informações falsas que comprometam a idoneidade do Hospital e do INDSH e* a assistência ao paciente.

DADOS PROFISSIONAIS

Nome: _____ Nº Matrícula/Conselho: _____

D. Nascimento: / / Função: _____ CPF: . . -

Empresa: ☐ INDSH ☐ Cooperativa:_____ Setor: _____

CEP: _____ Nº Residência: _____ Telefone: ( )

Confirmo que li e compreendo o que foi dito acima

Assinatura: _____ Data: / / Hora: :