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

Definir responsabilidades e orientar a conduta dos usuários de TI, visando a continuidade dos negócios através da confidencialidade, da integridade e da disponibilidade das informações do Complexo Hospitalar Zona Norte (CHZN).

2. DEFINIÇÕES E SIGLAS

PI – Política;
CHZN - Complexo Hospitalar Zona Norte
PSI - Política de Segurança da Informação;
TI – Tecnologia da Informação
CCO - Centro de Controle de Operações

3. 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!

3.1 DA ÁREA DE TI

Todos os chamados são recebidos pela TI INDSH, mas nem todos são solucionados por nossa equipe, necessitando ser direcionados às empresas parceiras da Tecnologia da Informação: AR RODRIGUEZ (contratado pelo próprio INDSH para dar suporte ao sistema DGS BRASIL), KONEC (empresa em TI contratada pela OZN - Opy Health) e o CCO (Empresa de manutenção a serviço da OZN - Opy Health).

Segue as atividades desenvolvidas por cada empresa:

3.1.2 TI AR RODRIGUEZ

- Criação de relatórios no sistema DGS BRASIL;
- Criação de documentos no sistema DGS BRASIL;
- Criação de formulários no sistema DGS BRASIL;
- Atualização do sistema DGS BRASIL;
- Gerenciamento do Servidor de aplicação e de dados do sistema DGS BRASIL;
- Capacitação de usuários no sistema DGS BRASIL;
- Gerenciamento de BI no sistema DGS BRASIL;
- Correções de falhas no sistema DGS BRASIL;
- Gerenciamento das integrações dos exames laboratoriais;
- Gerenciamento das integrações de imagem pelo aplicativo PAC.

3.1.3 CCO (Centro de controle e Operação)

- Manutenção de impressora;
- Instalação e troca de hardware e periféricos;
- Correção de falhas na rede interna e internet;
- Correções em computadores inoperantes.

3.1.4 TI INDSH

- Criação/ Bloqueio usuário no sistema DGS BRASIL;
- Auditoria de usuário no sistema DGS BRASIL;
- 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.

3.1.5 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 e Impressoras.

3.2 DOS USUÁRIOS:

- Respeitar esta Política de Segurança da Informação;
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Ativar suas senhas de proteção para correio eletrônico, sistema operacional e sistemas internos sob orientação do Gestor de Liberações da área de TI;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;
- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.;
- 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;
- Relatar para o seu responsável hierárquico e para o setor de TI o surgimento da necessidade de um novo software para suas atividades;
- 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.

4- DOS RESPONSÁVEIS HIERÁRQUICOS:

- Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- 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;
- Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberações da área de TI;
- Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI;
- Educar os usuários sobre os princípios e procedimentos de segurança da informação;
- Notificar imediatamente o gestor de liberações da área de TI, quaisquer vulnerabilidades e ameaças à quebra de segurança;
- Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;

- 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;
- Obter aprovação técnica do gestor de liberações da área de TI antes de solicitar a compra de hardware, software ou serviços de informática;
- Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

5. DESCRIÇÃO DA POLÍTICA

5.1 - 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.

5.2- ADMISSÃO E DEMISSÃO DE EMPREGADOS:

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

- 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;
- Comunicar sobre as rotinas a que os mesmos terão direito de acesso;
- 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.
- Todo ativo (informação) produzido pelo mesmo será mantido pelo INDSH garantindo o reconhecimento e o esclarecimento da propriedade do acervo para a instituição.

5.3- 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.

5.4- 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.

5.5- IDENTIFICAÇÃO - LOGIN E SENHA:

- Os sistemas de Login e senha protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra. Prevenindo a pratica de crime de Falsa Identidade previsto no art. 307 do Código Penal Brasileiro;
- 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;
- 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);
- 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;
- 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;
- Os usuários devem proceder a troca de senha caso suspeitem de quebra por terceiros;
    a) Os logins e senhas devem ser imediatamente bloqueados quando se tornarem desnecessários;
    b) Tentativa de violação e burla de senhas de acesso, criptografia ou identificação biométrica, se identificada, será alvo de medida disciplinar;

- 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.
- 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 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.

5.6- ACESSO A REDE COORPORATIVA E AO BANCO DE DADOS

Todo usuário para acessar os dados armazenados nos servidores do CHZN, deverá possuir um login e senha previamente cadastrados pela Tecnologia da Informação.

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.

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.

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.

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.

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.

5.7- RECURSOS COMPUTACIONAIS:

- Os recursos de TI alocados pelo CHZN aos seus usuários são destinados exclusivamente às atividades relacionadas ao trabalho;

- Quando o colaborador utilizar dispositivos de sua propriedade como ferramenta de trabalho no CHZN, seu uso será disciplinado por esta PSI;
- 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);
- Todo computador em desuso, deverá ser encaminhado a área de TI para a remoção das informações, descarte ou reuso.
- 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.

5.8- 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) Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;

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

5.9- DESCARTE DE MÍDIAS

- Mídias contendo informações referentes ao CHZN deverão ser destruídas antes de seu descarte ou guardadas em local seguro.
- 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.

6- 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.

7- ANTIVÍRUS

- A TI disponibiliza software corporativo de antivírus instalado para todos os usuários;
- O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor;
- 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.

8- ARMAZENAMENTO DE ARQUIVOS

- Todos os arquivos contidos nos servidores de rede ou nas estações de trabalho dos usuários devem ser exclusivamente de interesse do CHZN.
- É proibida a criação de pastas pessoais nos servidores de rede;
- 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;
- 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;
- 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.

9- SALVAGUARDA DE ARQUIVOS

- Compete ao gestor de continuidade da área TI criar e manter cópias de segurança (backups) apenas dos dados armazenados nos servidores de rede;
- 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;
- É de responsabilidade exclusiva do usuário a cópia de segurança (backup) e a guarda dos dados gravados da sua estação local de trabalho.

10- UTILIZAÇÃO DA REDE

- O CHZN possui uma rede integrada de computadores com servidores e um microcomputador para cada colaborador alocados na Unidade;
- 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;
- O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso;
- Os colaboradores do CHZN não deverão obter ou disponibilizar material sem a licença adequada através da rede;
- 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;
- O usuário está comprometido a utilizar a rede interna do CHZN para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence;
- É vedada a utilização de proxies que permitam o tráfego de informações a redes privadas externas;
- 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, tempestividade 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.

11- 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 abaixo descriminadas:

a) 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 STI (Setor de Tecnologia da Informação);

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

c) 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;

d) Não é permitido o acesso a sites de Internet com conteúdo pornográfico, 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;

e) 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.

f) 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;

g) A internet, via cabo ou Wi-Fi, deverá ser utilizada para fins profissionais, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades do CHZN;

h) 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.

Os colaboradores do CHZN não deverão:

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

- Acessar sites de pornografia, pedofilia 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.
- Os equipamentos fornecidos para o acesso à internet são de propriedade do CHZN 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.
- Assim, a organização, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.

12- 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.

13- 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.

14- 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.

15- 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 do 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.

16- UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS CORPORATIVOS

Dispositivos móveis corporativos são equipamentos portáteis dotados dec 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.

- É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações de uso interno, restritas ou confidenciais por meio de dispositivos móveis corporativos;
- 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;
- 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;
- Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel corporativo;
- 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;
- 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;
- 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);
- 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;

- 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;

17- 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.

18. 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.

18.1 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.

19- 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.

20- 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.

21- 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.
- 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.

22- ANEXOS

FO.CHZN.TI.699 - Termo de compromisso

23. 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 - Atualização norma ISO/IEC 27002:2013 para ISO/IEC 27002:2022
4. http://www.planalto.gov.br/ccivil_03/leis/l9279.htm
5. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12551.htm

24. HISTÓRICO DE REVISÕES

Não se aplica.

TERMO DE COMPROMISSO PARA USUÁRIOS DE ATIVOS DE TI

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

Termo de Compromisso

Declaro que li e estou de acordo com a *Política de Segurança da Informação* do CHZN e com o Manual de Padrões e 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 e a confidencialidade 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 nesta PSI.

PREENCHIMENTO SE FUNCIONÁRIO:

Nome:_____

CPF ou RG:_____ **Telefone ( )**_____

Setor:_____ **Função:**_____

Data de admissão: _____/_____/_____ **Nº Matrícula:**_____

PREENCHIMENTO SE PRESTADOR DE SERVIÇOS/PARCEIRO

Nome:_____

CPF ou RG:_____ **Telefone ( )**_____

Empresa:_____ **Função:**_____

Data de admissão: _____/_____/_____ **Nº Matrícula:**_____

Data: _____/_____/_____

Assinatura: _____