COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO – CGTI
POLITICA DE SEGURANÇA DA INFORMAÇÃO (PSI)
DIRETRIZES E NORMAS ADMINISTRATIVAS

DEPARTAMENTO DE GESTÃO DA TECNOLOGIA DE INFORMAÇÃO

INTRODUÇÃO

A Santa Casa de Misericórdia de Casa Branca é corresponsável junto a eventuais terceiros contratados pelo armazenamento e processamento de informações de diversos segmentos da municipalidade seja em Data Centers existentes e Cloud's (computação em nuvens) devendo processar e disponibilizar essas informações adequadamente e protegê-las contra ameaças e riscos

Políticas, normas e procedimentos que visem garantir a segurança da informação devem ser prioridades constantes da Santa Casa de Misericórdia de Casa Branca, reduzindo-se os riscos de falhas, os danos e os prejuízos que possam comprometer sua imagem e seus objetivos.

A Política de Segurança da Informação (PSI) define as diretrizes, os limites e o direcionamento que a prefeitura deseja, para os controles que serão implantados na proteção de suas informações e a responsabilidade legal de todos os colaboradores e usuários, devendo ser cumprida e aplicada em todas as áreas da administração direta e indireta.

Uma política de segurança da informação (PSI) ou PoSIC (Política de Segurança das Informações e Comunicações) que tem por objetivo possibilitar o gerenciamento da segurança em uma organização, estabelecendo regras e padrões para proteção da informação. A política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário.

A segurança da informação procura proteger diferentes tipos de ameaças para garantir a continuidade dos negócios, reduzir riscos e busca a maximização dos retornos em investimentos e ampliação das oportunidades de negócios.

Política de segurança da informação é a padronização das normas obrigatórias a fim de manter o controle do comportamento dos envolvidos para garantir a proteção e as informações da organização. Se tornando semelhante ao Direito, as leis possuem em si definição semelhante as políticas de segurança da informação, e para a avaliação de eficiência e eficácia de uma PSI, quanto a manutenção comportamental, é indicado uma adaptação das teorias de análise comportamental do Direito.

A segurança da informação visa manter a proteção contra diferentes tipos de ameaças para garantir a continuidade dos negócios, reduzir riscos e busca a maximização dos retornos em investimentos e ampliação das oportunidades de negócios.

Política de segurança da informação é a padronização das normas obrigatórias a fim de manter o controle do comportamento dos envolvidos para garantir a proteção e as informações da organização. Se tornando semelhante ao Direito, as leis possuem em si definição semelhante as políticas de segurança da informação, e para a avaliação de eficiência e eficácia de uma PSI, quanto a manutenção comportamental, é indicado uma adaptação das teorias de análise comportamental do Direito.

Esta PSI baseia-se nas recomendações propostas pela norma técnica ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está em conformidade com as leis vigentes em nosso país.

1. OBJETIVO:

Resultar na documentação dos procedimentos criados por essa política e sua padronização, também suas ferramentas e técnicas utilizadas. Criando assim indicadores, registros e definindo um processo de conscientização.

Definir o tratamento a ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional e no ambiente de tecnologia da Santa Casa de Misericórdia de Casa Branca.

Estabelecer e definir normas, processos, procedimentos e controles específicos de segurança da informação, bem como implementá-los.

Preservar as informações quanto à:

1.1 Confidencialidade – Toda informação deve ser acessada por quem de direito, até que se torne pública. Assegurar que informações confidenciais e críticas não sejam subtraídas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas;

1.2 Integridade: preservação da precisão, consistência e confiabilidade das informações e sistemas;

1.3 Disponibilidade: Garantia de acesso à informação durante o ciclo de sua existência;

1.4 Conformidade: Toda informação deve estar em conformidade com os padrões, regras e especialmente com a legislação vigente;

1.5 Auditabilidade: Configuração de sistemas e bases de dados de forma a possibilitar o rastreamento de atividades físicas e lógicas.

2. ESTRUTURA:

2.1 Política de Segurança da Informação (Política): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;

2.2 Normas de Segurança da Informação (Normas): estabelecem obrigações e procedimentos definidas de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;

2.3 Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da Santa Casa de Misericórdia de Casa Branca.

3. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA:

A Política e as Normas de Segurança da Informação serão divulgadas a todos os colaboradores da Santa Casa de Misericórdia de Casa Branca âmbito da administração direta e indireta e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento, utilizando a intranet e outros canais apropriados. Os Procedimentos de Segurança da Informação serão divulgados às áreas diretamente relacionadas à sua aplicação.

4. APROVAÇÃO E REVISÃO:

Os documentos integrantes da estrutura normativa da Segurança da Informação da Santa Casa de Misericórdia de Casa Branca serão aprovados e revisados quando motivados por algum fato relevante ou evento, e também conforme os seguintes critérios.

4.1 Política:

4.1.1 Nível de Aprovação: Comitê Gestor de Tecnologia da Informação – CGTI;

4.1.2 Periodicidade de Revisão: anual.

5. ABRANGÊNCIA:

5.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da administração direta e indireta que utilizam ou geram as informações da Santa Casa de Misericórdia de Casa Branca;

5.2. Os colaboradores dos organismos da administração indireta, empresas, autarquias, fundações e afins, atenderão pelo menos o disposto neste Decreto, podendo referidos organismos estabelecerem instrumentos próprios, se aprovados nas suas instâncias.

6. PRINCÍPIOS:

6.1. Toda informação, produzida ou recebida pelos colaboradores como resultado da atividade profissional, pertence à Santa Casa de Misericórdia de Casa Branca;

6.2. Todos os equipamentos, sistemas e informações devem ser utilizados pelos colaboradores para a realização das atividades profissionais. O uso dos mesmos com finalidade pessoal, é proibido;

6.3. Esta PSI dá ciência a cada colaborador de que os ambientes, sistemas, dispositivos informáticos e redes, no âmbito da administração direta e indireta, poderão ser monitorados e gravados, conforme previsto nas leis

brasileiras, Inciso III do Artigo 932 da Lei nº 10.406 de 10 de janeiro de 2002;

6.4. Todas as informações que estiverem sob responsabilidade de terceiros devem ser disponibilizadas periodicamente de forma clara e identificável todas as relações dos campos, assegurando que a gestão consiga dar continuidade nas operações sem a perda das produções;

6.5. Caso o item 6.4 não possa ser atendido a empresa terceira deverá disponibilizar as informações através de backups (cópia do banco de dados ou em planilhas eletrônicas ou arquivos CSV) e dicionário de dados.

7. REQUISITOS:

7.1. A PSI será comunicada a todos os colaboradores e terceiros da Santa Casa de Misericórdia de Casa Branca, com a finalidade de que seja cumprida dentro e fora da mesma;

7.2. É obrigação de cada colaborador e terceiros manterem-se atualizados em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação de seus superiores imediatos sempre que não estiverem absolutamente seguros quanto à aquisição, uso ou descarte de informações;

7.3. A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores. Todos os colaboradores serão orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos, devendo assinar o termo de responsabilidade constante no ANEXO I deste documento;

7.4. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao superior imediato;

7.5. A Santa Casa de Misericórdia de Casa Branca exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores e terceiros, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios de natureza civil, administrativa e criminal, bem como adotar as medidas legais cabíveis;

7.6. Esta PSI será implementada na Santa Casa de Misericórdia de Casa Branca por meio de procedimentos específicos, obrigatórios para todos os colaboradores e terceiros, independentemente de nível hierárquico, função ou vínculo empregatício daqueles que terão acesso a seus sistemas e equipamentos;

7.7. O não cumprimento dos requisitos previstos nesta PSI e demais instrumentos normativos complementares, acarretará violação às regras internas da administração municipal e sujeitará o usuário às medidas administrativas e legais cabíveis.

8. ATRIBUIÇÕES E RESPONSABILIDADES.

8.1. Comitê Gestor de Tecnologia da Informação – CGTI. Cabe ao CGTI:

8.1.1. Aprovar a Política de Segurança da Informação e suas revisões;

8.1.2. Aprovar e nomear os administradores da informação;

8.1.3. Tomar as decisões administrativas referentes aos casos de descumprimento da Política e de suas Normas.

8.2. Grupo Técnico Executivo do Comitê Gestor de Informática (GTECGI).

Cabe ao GTECGI:

8.2.1. Propor ajustes, aprimoramentos e modificações desta Política;

8.2.2. Propor melhorias e aprovar as Normas de Segurança da Informação;

8.2.3. Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando à CGTI;

8.2.4. Propor projetos e iniciativas relacionados à melhoria da segurança da informação da Prefeitura Municipal de Casa Branca;

8.2.5. Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;

8.2.6. Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;

8.2.7. Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;

8.2.8. Propor a relação de administradores das informações da Santa Casa de Misericórdia de Casa Branca;

8.2.9. De acordo com a necessidade, qualquer funcionário da Santa Casa de Misericórdia de Casa Branca convidado externo poderá participar das reuniões do GTECGI;

8.2.10. Caberá ao Secretário Executivo do CGTI a coordenação dos trabalhos do GTECGI, cujas atribuições abrangerão a convocação das reuniões e a realização de outros atos de suporte às atividades desenvolvidas;

8.2.11. As reuniões do GTECGI:

8.2.11.1. Serão realizadas semestralmente referente ao assunto PSI, podendo haver convocação extraordinária sempre que necessário;

8.2.11.2. Deverão ser registradas em ata. O GTECGI deliberará por maioria dos votos presentes.

8.3. Interlocutores da Segurança de Informação dos Setores (ISIS).

Com a responsabilidade de divulgar, atualizar e difundir a Política de Segurança de Informação entre seus pares nos Setores, serão indicados os Interlocutores da Segurança de Informação dos Setores (ISIS).

Cada Diretor de setor indicará 1 (um) Interlocutor da Segurança de Informação (ISI), o qual será parte integrante do Grupo Técnico Executivo do Comitê Gestor de Informática (GTECGI).

Caberá aos ISIS:

8.3.1. Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores de seu setor ou órgão da administração direta e indireta;

8.3.2. Oferecer orientação sobre a Política de Segurança da Informação e suas Normas a todos os colaboradores de seu setor ou órgão da administração direta e indireta;

8.3.3. Analisar os riscos relacionados à segurança da informação da Santa Casa de Misericórdia de Casa Branca;

8.3.4. Apresentar relatórios sobre tais riscos ao GTECGI e ao CGTI;

8.3.5. Estabelecer mecanismo para registro e controle de infrações à PSI e comunicar essas infrações ao GTECGI e ao CGTI.

8.4. Administrador da Informação.

O administrador da informação é um colaborador da Santa Casa de Misericórdia de Casa Branca, formalmente indicado setores que será responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à Santa Casa de Misericórdia de Casa Branca ou sob a sua guarda.

Cabe ao administrador da informação:

8.4.1. Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da Santa Casa de Misericórdia de Casa Branca às autorizações de acesso concedidas;

8.4.2. Autorizar a liberação de acesso à informação sob sua responsabilidade, as liberações, observadas a matriz de cargos e funções,

a Política e as Normas de Segurança da Informação da Santa Casa de Misericórdia de Casa Branca e as diretrizes específicas do CGTI;

8.4.3. Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;

8.4.4. Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;

8.4.5. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

8.4.6. Participar, sempre que convocado, das reuniões do CGTI ou GTECGI, prestando os esclarecimentos solicitados;

8.4.7. Inativar de pronto o acesso aos sistemas do órgão, quando da saída de colaboradores de sua área de responsabilidade.

8.5. Setores.

Cabe aos Gestores principais dos Setores:

8.5.1. Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

8.5.2. Assegurar que suas equipes possuam acesso e conhecimento desta Política, das Normas e dos Procedimentos de Segurança da Informação;

8.5.3. Sugerir os Procedimentos de Segurança da Informação relacionados às suas áreas;

8.5.4. Comunicar imediatamente eventuais casos de violação de segurança da informação ao CGTI e GTECGI.

8.6. Setor de Administração.

Cabe à Setor de Administração:

8.6.1. Colher a assinatura do Termo de Responsabilidade dos funcionários, estagiários e terceirizados, arquivando-o nos respectivos prontuários;

8.6.2. Tomar as providências administrativas no caso de aplicação de penalidades aos trabalhadores quanto ao não cumprimento da Política de Segurança da Informação.

8.7 Todos os Colaboradores.

Entende-se por colaborador toda e qualquer pessoa física, contratada ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da Instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à Santa Casa de Misericórdia de Casa Branca ou à terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Cabe aos Colaboradores:

8.7.1. Cumprir as normas definidas na Política de Segurança;

8.7.2. Reportar, de imediato, ao superior hierárquico, qualquer incidente de segurança ou, até mesmo, suspeitas iminentes;

8.7.3. Sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação.

8.8 COLABORADORES EM REGIME DE EXCEÇÃO (TEMPORÁRIOS).

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no Termo de Responsabilidade concedido pela Santa Casa de Misericórdia de Casa Branca.

A concessão poderá ser revogada a qualquer tempo, se for verificada que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção, ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no termo.

9. NORMAS GERAIS.

9.1. Monitoramento e Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, a Santa Casa de Misericórdia de Casa Branca poderá:

9.1.1. implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas será usada para identificar usuários e respectivos acessos efetuados, bem como o material manipulado;

9.1.2. tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, processo administrativo, solicitação do gestor do setor ou órgão, ou superior hierárquico;

9.1.3. realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

9.1.4. instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

9.2. Correio Eletrônico.

O uso do correio eletrônico da Santa Casa de Misericórdia de Casa Branca é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. É vedado o uso do correio eletrônico da Santa Casa de Misericórdia de Casa Branca, para fins pessoais e o uso do correio eletrônico particular e pessoal para fins de atividades dentro da instituição.

Acrescentamos que é proibido o uso do correio eletrônico para:

9.2.1. (SPAM) enviar sem autorização mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao legítimo interesse da prefeitura;

9.2.2. Enviar sem autorização mensagens pelo endereço de seu departamento ou usando o nome ou endereço de correio eletrônico de outra pessoa;

9.2.3. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente, a Santa Casa de Misericórdia de Casa Branca, ou suas unidades, vulneráveis a ações cíveis ou criminais;

9.2.4. Divulgar sem autorização da Chefia da Seção ou Departamento relacionados, qualquer informação ou imagem de tela de sistemas, documentos e afins, as quais não sejam estritamente relacionadas ao requerente em questão;

9.2.5. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes ou destinatários, com o objetivo de evitar as punições previstas;

9.2.6. Apagar mensagens pertinentes de correio eletrônico institucional quando a Santa Casa de Misericórdia de Casa Branca estiver sujeita a algum tipo de investigação ou mudança de setor;

9.2.7. Produzir, transmitir ou divulgar mensagem ou imagem que:

9.2.7.1. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Santa Casa de Misericórdia de Casa Branca;

9.2.7.2. Contenha ameaças eletrônicas, como: spam6, mail bombing7, vírus de computador e etc.;

9.2.7.3. Contenha arquivo executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src,. cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

9.2.7.4. Intencional a obter acesso não autorizado a outro computador, servidor ou rede;

9.2.7.5. Intencional a interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

9.2.7.6. Intencional a burlar qualquer sistema de segurança;

9.2.7.7. Intencional a vigiar secretamente ou assediar outro usuário;

9.2.7.8. Intencional a acessar informações confidenciais sem explícita autorização do proprietário;

9.2.7.9. Intencional a acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

9.2.7.10. Inclua imagens criptografadas ou de qualquer forma mascaradas;

9.2.7.11. Contenha conteúdo considerado impróprio, obsceno ou ilegal;

9.2.7.12. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;

9.2.7.13. Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

9.2.7.14. Tenha fins políticos locais ou do país (propaganda política);

9.2.7.15. Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

9.2.8. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

9.2.8.1. Nome do colaborador;

9.2.8.2. Setor/Departamento;

9.2.8.3. Santa Casa de Misericórdia de Casa Branca;

9.2.8.4. Telefone (s);

9.2.8.5. Correio eletrônico, fica restringido o uso de e-mails pessoais.

9.3. INTERNET E INTRANET:

9.3.1. Todas as regras atuais da Santa Casa de Misericórdia de Casa Branca visam o desenvolvimento de um comportamento ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação;

9.3.2. Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Santa Casa de Misericórdia de Casa Branca, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela;

9.3.3. Os equipamentos, tecnologia e serviços fornecidos para o acesso à

internet são de propriedade da Santa Casa de Misericórdia de Casa Branca, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede ou internet, estejam eles em disco local, na estação de trabalho ou em áreas privadas da rede, visando assegurar o cumprimento de sua PSI;

9.3.4. A Santa Casa de Misericórdia de Casa Branca ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e superior imediato. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes;

9.3.5. Somente os colaboradores que estão devidamente autorizados a se manifestar em nome da Santa Casa de Misericórdia de Casa Branca (exemplo Provedor, Secretários, Assessoria de Comunicação, Titulares da Administração Indireta, etc.) para os meios de comunicação, poderão manifestar-se, seja por e-mail, entrevista on-line, Podcast, seja por documento físico, entre outros;

9.3.6. Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais;

9.3.7. É proibida a divulgação ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet;

9.3.8. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos;

9.3.9. Os colaboradores não poderão em hipótese alguma utilizar os recursos da Santa Casa de Misericórdia de Casa Branca para efetuar o download ou distribuição de software ou dados não licenciados ou ilegais, atividade considerada delituosa de acordo com a legislação nacional;

9.3.10. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidas pelos respectivos superiores imediatos, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção;

9.3.11. Colaboradores com acesso à internet não poderão efetuar upload ou cópia de qualquer software licenciado à Santa Casa de Misericórdia de Casa Branca ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados;

9.3.12. Os colaboradores não poderão utilizar os recursos da Santa Casa de Misericórdia de Casa Branca para deliberadamente propagar qualquer tipo de vírus, worm9, cavalo de troia, spam, assédio, constrangimento ou programas para controle de outros computadores;

9.3.13. Já os serviços de streaming (rádios on-line, canais de broadcast e afins), comunicação instantânea (Gtalk, Skype, WhatsApp e afins) e redes sociais (Facebook, LinkedIn e afins) poderão ser permitidos em regime de exceção quando formalmente autorizado pelos Interlocutores de Segurança de Informação Setores;

9.3.14. Nos períodos eleitorais, é proibido o uso de quaisquer equipamentos aqui abrangidos e das redes de comunicação da administração nos âmbitos da administração direta e indireta, por qualquer colaborador, para fins eleitorais;

9.3.15. Não é permitido o acesso à internet por meio de proxy não autorizado pela Santa Casa de Misericórdia de Casa Branca;

9.3.16. A Intranet será alimentada por informações produzidas pela administração direta e indireta seguindo, no que couber, os mesmos critérios aplicados acima para a internet.

9.4. Política De Senhas:

9.4.1. Os dispositivos de identificação com senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Santa Casa de Misericórdia de Casa Branca ou terceiros;

9.4.2. O uso de acessos, com identificação de outra pessoa, constitui crime tipificado no Código Penal Brasileiro (art. 307 – Falsidade Ideológica);

9.4.3. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores;

9.4.4. Todo e qualquer sistema de identificação pessoal, em hipótese alguma, poderá ser compartilhado com outras pessoas;

9.4.5. A Administração da Santa Casa de Misericórdia de Casa Branca é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores. Os administradores da informação respondem pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários;

9.4.6. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas;

9.4.7. Os usuários que não possuem perfil de administrador 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) sempre que possível;

9.4.8. Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (# $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente;

9.4.9. 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;

9.4.10. As senhas não devem ser salvas em navegadores nem anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem se basear em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da organização, nome do

departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, “q1w2e3″entre outras;

9.4.11. Após 3 (três) tentativas de acesso sem sucesso, a conta do usuário será bloqueada, caso o ambiente acessado permita esse procedimento. Para o desbloqueio é necessário que o usuário entre em contato com o Administrador da Informação. Em alguns casos o bloqueio poderá ser temporário (por exemplo 10 minutos), e após esse tempo o usuário é desbloqueado automaticamente;

9.4.12. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

9.4.13. Os usuários devem alterar sua senha em caso de suspeita de que terceiros tenham obtido acesso à sua conta;

9.4.14. O sistema poderá solicitar a troca da senha a cada 180 dias;

9.4.15. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários;

9.4.16. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca por meio de chamado técnico.

9.5. Acesso Remoto Externo.

9.5.1. Objetivo:

9.5.1.1. Estabelecer critérios para a disponibilização do serviço de acesso remoto externo à rede corporativa da Santa Casa de Misericórdia de Casa Branca, bem como as regras para a sua utilização, visando a prevenção do acesso não autorizado às informações.

9.5.2. Diretrizes Gerais:

9.5.2.1. O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores que, oficialmente, executem atividade vinculada à atuação institucional da Santa Casa de Misericórdia de Casa Branca e que necessitam deste serviço para execução de suas atividades institucionais, desde que autorizados;

9.5.2.2. A liberação de acesso remoto, só será efetivada após avaliação e aprovação pelo ISIS, para que se evitem ameaças à integridade e sigilo das informações contidas na rede corporativa da Santa Casa de Misericórdia

de Casa Branca. Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança do ambiente;

9.5.2.3. A solicitação do acesso remoto deve conter, no mínimo, as seguintes informações:

9.5.2.3.1. Data da solicitação;

9.5.2.3.2. Tipo de solicitação;

9.5.2.3.3. Tempo de validade do acesso remoto;

9.5.2.3.4. Justificativa;

9.5.2.3.5. Dados do solicitante;

9.5.2.3.6. Dados do usuário.

9.5.2.4. Será disponibilizado formulário eletrônico via intranet para solicitação e controle do Acesso Remoto;

9.5.2.5. A disponibilização de acesso remoto à rede corporativa da Santa Casa de Misericórdia de Casa Branca para outras organizações deve obedecer às seguintes regras:

9.5.2.5.1. Direitos de acesso definidos por convenio formal entre as partes;

9.5.2.5.2. Acesso temporário e limitado às necessidades de negócio;

9.5.2.5.3. Revisão periódica dos direitos de acesso;

9.5.2.5.4. Utilização de solução que permita a implementação e controle de regras de acesso;

9.5.2.6. O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

9.5.2.6.1. Finalização do período especificado na solicitação ou contrato;

9.5.2.6.2. Perda da necessidade de utilização do serviço;

9.5.2.6.3. Transferência do usuário para outras unidades;

9.5.2.6.4. Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.

9.5.2.7. As conexões remotas à rede corporativa da Santa Casa de Misericórdia de Casa Branca devem ocorrer da seguinte maneira:

9.5.2.7.1. Utilização de autenticação;

9.5.2.7.2. As senhas e as informações que trafegam entre a estação remota e a rede corporativa da Santa Casa de Misericórdia de Casa Branca devem estar criptografadas;

9.5.2.7.3. Todas as conexões e acessos poderão ser registrados em log, para posterior auditoria;

9.5.2.8. Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não o fornecer a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas;

9.5.2.9. É vedada a utilização do acesso remoto para fins não relacionados às atividades da prefeitura.

9.6. Computadores, Dispositivos Portáteis e Recursos Tecnológicos:

9.6.1. A Santa Casa de Misericórdia de Casa Branca é detentora dos equipamentos fornecidos, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da prefeitura, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis;

9.6.2. A Santa Casa de Misericórdia de Casa Branca reserva-se ao direito de inspecionar qualquer equipamento que estiver a serviço da instituição a qualquer momento;

9.6.3. É proibido qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um ISI, ou de quem este determinar;

9.6.4. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos deverão ser realizadas constantemente, entretanto somente após a sua disponibilização oficial do fabricante ou fornecedor;

9.6.5. Os computadores e dispositivos portáteis que são propensos a falha de segurança grave, deverão ter versões do software antivírus instalados e ativados permanentemente, mantendo-os atualizados. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no Departamento de Gestão de Tecnologia da Informação ou terceiro, conforme contrato;

9.6.6. A transferência ou a divulgação de qualquer informação, software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a identificação positiva do solicitante junto ao Gestor responsável por esta informação, e estando de acordo com a classificação dessa informação e a pertinente necessidade do destinatário;

9.6.7. Ao transportar computador ou dispositivo portátil em veículos motorizados, o mesmo deverá ser colocado sempre no interior do porta-malas ou local onde não ficará visível, não o deixando no interior do veículo quando ele estiver estacionado.

9.7. Uso dos Equipamentos:

9.7.1. No uso dos computadores, dispositivos móveis, equipamentos e recursos de informática, algumas regras devem ser atendidas;

9.7.2. Todos os computadores de uso individual deverão ter o BIOS protegido por meio de senha, com o objetivo de restringir o acesso de pessoas não autorizadas. Tais senhas serão definidas pelo Departamento de Gestão de Tecnologia da Informação, conforme contrato, que terá acesso a elas para manutenção dos equipamentos;

9.7.3. Os colaboradores devem informar ao ISI – Interlocutores de Segurança da Informação, qualquer identificação de dispositivo estranho conectado ao seu computador;

9.7.4. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico interno ou por terceiros devidamente contratados para o serviço;

9.7.5. É proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;

9.7.6. O colaborador deverá manter a configuração do equipamento disponibilizado pela Santa Casa de Misericórdia de Casa Branca, seguindo os devidos controles de segurança exigidos pela PSI e pelas normas específicas da instituição, assumindo a responsabilidade das informações e utilização;

9.7.7. Devem na ausência prolongada tomar medidas para a economia de energia e ao final do expediente devem ser desligados;

9.7.8. Todos os recursos tecnológicos adquiridos pela Santa Casa de Misericórdia de Casa Branca devem ter imediatamente suas senhas padrão alteradas;

9.7.9. Os equipamentos deverão manter preservados em modo seguro, os registros de eventos, constando identificação dos usuários, datas e horários de acesso;

9.7.10. É proibido o uso de computadores e recursos tecnológicos da Santa Casa de Misericórdia de Casa Branca para:

9.7.11. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

9.7.12. Burlar quaisquer sistemas de segurança;

9.7.13. Acessar informações confidenciais sem explícita autorização do proprietário;

9.7.14. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

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

9.7.16. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio, constrangimento, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

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

9.8 Dispositivos Portáteis:

9.8.1. Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados do dispositivo móvel pertencente a Santa Casa de Misericórdia de Casa Branca sob sua guarda. Deverá, também, manter esses backups em local diferente de sua fonte de origem;

9.8.2. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes;

9.8.3. Os dispositivos móveis que permanecerem em qualquer área física da Santa Casa de Misericórdia de Casa Branca deverão estar trancados em local de acesso restrito e seguro, quando não estiverem sendo utilizados pelo usuário;

9.8.4. Ao viajar com um computador tipo portátil, o usuário deve:

9.8.4.1. Manter o computador tipo portátil sempre consigo;

9.8.4.2. Ao utilizar todo e qualquer meio de transporte público no deslocamento em função de atividade de trabalho (ônibus, avião, carros através de aplicativos, ou outros enquadramentos), dentro ou fora do município, desde que autorizado, certificar-se de que retirou toda a sua bagagem, inclusive o computador e demais equipamentos, quando chegar em seu destino final;

9.8.5. O transporte do computador tipo portátil nas ruas é bastante observado pelos criminosos, portanto, é aconselhável discrição e atenção no ambiente e seus arredores no trajeto até o seu destino;

9.8.6. Em caso de perda de acessório (exemplo: mala, capa, mouse e etc.) o colaborador será responsável pelo seu ressarcimento, em igual ou superior especificação, qualidade ou finalidade;

9.8.7. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Santa Casa de Misericórdia de Casa Branca notificar imediatamente seu gestor direto. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO);

9.8.8. O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel não é permitido. Caso haja conclusão de que houve uso indevido, o mesmo será responsabilizado conforme legislação vigente.

9.9. Uso da Rede:

9.9.1. Arquivos pessoais ou não pertinentes aos assuntos da Santa Casa de Misericórdia de Casa Branca (fotos, músicas, vídeos, etc.) não poderão ser copiados ou movidos para a rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente, sem aviso prévio;

9.9.2. Diretórios ou pastas de acesso público, não deverão ser utilizados para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica. Devem ser utilizados apenas para armazenar informações de interesses gerais, ou para transferência de informações entre diferentes usuários;

9.9.3. Arquivos em geral (textos, planilhas, imagens, vídeos e outros) que estejam duplicados na rede, e os que não forem de interesse da administração, serão excluídos por auditoria periódica na rede;

9.9.4. Arquivos e documentos imprescindíveis para as atividades e produção dos colaboradores na Santa Casa de Misericórdia de Casa Branca deverão ser salvos em computadores de repositórios nos departamentos ou em servidores externos e os backups deverão ser salvos em dispositivos externos;

9.9.5. Os colaboradores da Santa Casa de Misericórdia de Casa Branca no âmbito da administração direta e indireta e detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que possa sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização;

9.10. Engenharia Social:

9.10.1. A engenharia social é qualquer método usado para enganar ou explorar a confiança das pessoas para a obtenção de informações sigilosas e importantes, tanto da instituição como do colaborador em questão. Para isso, alguém pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área e etc.;

9.10.2. Para evitar esse método, todos os colaboradores devem estar cientes das seguintes regras:

9.10.2.1. Nenhum colaborador da instituição está autorizado a passar informação às pessoas ou agentes estranhos dentro da prefeitura;

9.10.2.2. Caso alguém entre em contato por telefone, e-mail, softwares de comunicação, solicitando informações sigilosas da prefeitura ou do usuário, o colaborador abordado deverá entrar em contato com o responsável da rede interna, ou diretamente com seu superior hierárquico informando tais situações;

10. CONCLUSÃO.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura da Santa Casa de Misericórdia de Casa Branca. Ou seja, qualquer incidente de segurança, entender-se-á como alguém agindo contra a ética e os bons costumes regidos pela prefeitura. O não cumprimento desta PSI e demais instrumentos normativos que complementam o processo de segurança constitui falta grave, e o colaborador estará sujeito às penalidades administrativas, contratuais, cíveis e criminais, conforme a legislação vigente.

11. GLOSSÁRIO

- **Data Center:** É o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma organização.

- **Colaborador:** Toda e qualquer pessoa física, contratada, concursada ou comissionada ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da administração direta ou indireta da Santa Casa de Misericórdia de Casa Branca.

- **Dispositivo Informático:** Qualquer equipamento que processa, transmite ou armazena informação (computador, HD, pen drive, impressora, modem e etc.).

- **Ativos de informação:** São informações potencialmente valiosas.

- **Proprietário da informação:** É o responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações.

- **Spam:** significa uma mensagem eletrônica não-solicitada geralmente enviada em massa.

- **E-mail Bombing:** consiste em enviar milhares de mensagens para uma caixa de correio eletrônico para sobrecarregar um servidor ou uma conta de e-mail.

- **Podcast:** é uma forma de publicação de arquivos de áudio pela Internet que permite aos utilizadores acompanhar a sua atualização.

- **Worm:** é um programa autorreplicante, diferente de um vírus.

- **Peer-to-peer ou P2P:** consiste num conjunto de computadores que comunicam entre si de forma descentralizada, isto é, são nós centrais responsáveis por gerir as ligações entre eles sem a necessidade de um centralizador (servidor). É muito utilizado para compartilhamento de arquivos.

- **Streaming:** é frequentemente utilizada para distribuir conteúdo multimídia por meio da Internet.

- **Proxy:** é um servidor intermediário, nesse caso tornando possível o acesso à internet a partir de uma máquina externa.

- **Dispositivos portátil ou móvel:** é qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou pessoal aprovado e permitido por sua Gerência de Infraestrutura e Suporte, como: notebooks, tablets, smartphones e pendrives.

- **Classificação da Informação:** é o modo de determinar como esta informação vai ser tratada e protegida durante todo o seu ciclo de vida.

- **BIOS:** é um programa de computador pré-gravado em memória permanente (firmware) executado por um computador quando ligado. Ele é responsável pelo suporte básico de acesso ao hardware, bem como por iniciar a carga do sistema operacional.