



GERÊNCIA DE INFORMÁTICA

NORMAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Sumário

1.	Introdução	3
2.	Responsabilidades da Área de Tecnologia da Informação.....	4
2.1	Da Gerência de Informática	4
2.2	Monitoramento e Auditoria do Ambiente	4
3.	Manual de Normas e Procedimentos de Segurança da Informação	5
3.1	Objetivo:.....	5
3.2	Finalidade dos Recursos Computacionais:	5
3.3	Classificação da Informação:.....	5
3.5	Direito à Propriedade:.....	5
3.6	Regras de Utilização	6
	I. Correio Eletrônico (e-mail):	6
	III. Recursos de Rede	7
	IV. Armazenamento de Arquivos	8
	V. Internet	9
	VI. Rede Sem Fio (WiFi)	10
3.7	Penalidades	11
4.	ATIVIDADES NÃO PERMITIDAS E SUAS RECOMENDAÇÕES.....	11

1. Introdução

Este documento serve de complemento da Política e Segurança da Informação (PSI) da instituição, tendo por finalidade apresentar normas regulamentadas pelo Comitê Gestor da Política e Segurança da Informação do GHC – CGPSI/GHC, e descrever as definições dos procedimentos utilizados pela Gerência de Informática do Grupo Hospitalar Conceição (GI/GHC) para cumprir com os objetivos propostos na PSI . Além disso, busca atender a Instrução Normativa GSI/PR nº1, de 13 de junho de 2008, e apresentar os mecanismos utilizados pela instituição para cumprir com as instruções do Marco Cível da Internet (Lei nº: 12.965).

2. Responsabilidades da Área de Tecnologia da Informação

2.1 Da Gerência de Informática

A Gerência de Informática é o setor competente para esclarecer eventuais dúvidas, aplicar e orientar quanto à aplicação da Política de Segurança da Informação do Grupo Hospitalar Conceição (GHC).

2.2 Monitoramento e Auditoria do Ambiente

A Gerência de Tecnologia da Informação pode, a qualquer tempo:

- a) Monitorar e registrar dados como início e fim de conexões à rede, tempo de CPU, utilização de discos feita por usuário, registros de auditoria, carga de rede, dentre outros.
- b) Monitorar e registrar o uso de determinados recursos como servidores, estações de trabalho, rede, modems, impressoras, etc.
- c) Havendo evidência de atividade que possa comprometer a segurança da rede ou dos computadores, monitorar as atividades e acessos de um determinado recurso, além de inspecionar arquivos, a bem do interesse da organização.
- d) Suspender todos os privilégios de determinado usuário em relação ao uso de redes e computadores sob sua responsabilidade, por razões ligadas à segurança física e ao bem-estar dos usuários, ou por razões disciplinares ou relacionadas à Segurança da Informação e ao bem-estar dos outros membros da rede.

3. Manual de Normas e Procedimentos de Segurança da Informação

3.1 Objetivo:

Definir responsabilidades e orientar a conduta dos profissionais e usuários de informática do GHC na utilização dos recursos computacionais, visando garantir a integridade, disponibilidade, valor e confidencialidade das informações.

3.2 Finalidade dos Recursos Computacionais:

Os recursos de tecnologia de informação disponibilizados pelo GHC são destinados exclusivamente às atividades da instituição.

3.3 Classificação da Informação:

O GHC adotou os seguintes níveis de classificação da Informação:

Pública - Esta informação é de acesso irrestrito, podendo ser utilizada por todos sem causar danos à organização;

Interna – Tipo de informação que o GHC não tem interesse em divulgar, cujo acesso por parte de indivíduos externos a ela deve ser evitado. Entretanto, caso esta informação seja disponibilizada ela não causa danos sérios à organização. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços do GHC;

Confidencial - Informação interna do GHC, cuja divulgação pode causar danos operacionais ou à imagem da instituição ou, ainda, passível de sanções administrativas, civis e criminais. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores;

Secreta – Informação interna, restrita a um grupo seleto dentro do GHC. Sua integridade deve ser preservada a qualquer custo e o acesso bastante limitado e seguro. Esta é a informação considerada vital para a companhia.

3.5 Direito à Propriedade:

Os programas homologados e instalados nos computadores e nos servidores de rede são propriedade exclusiva do GHC, sendo vetada sua cópia parcial ou integral.

São de propriedade da instituição, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com o GHC.

3.6 Regras de Utilização

I. Correio Eletrônico (e-mail):

O serviço de correio eletrônico (e-mail) disponibilizado pelo GHC é ferramenta de trabalho proporcionada pela instituição aos seus colaboradores para realização de seus serviços e estão sujeitos a violabilidade amostral e/ou mediante processo administrativo disciplinar, portanto, deverá ser usado para comunicações corporativas de interesse do GHC sem infringir as leis brasileiras ou os aspectos morais e éticos vigentes na instituição. As mensagens de correio eletrônico interno estão permanentemente sujeitas ao rastreamento como forma de identificar o envio/recebimento de mensagens com conteúdo pornográfico e/ou indesejados. O mesmo vale para arquivos anexos.

GHC fornecerá, a seu critério, contas de correio eletrônico (@ghc.com.br) aos seus funcionários.

GroupWise é o software oficial utilizado pelo GHC para troca de mensagens por e-mail e pode ser acessado via versão web através do endereço eletrônico <https://correio.ghc.com.br/gw/webacc>;

Cada usuário poderá solicitar um endereço eletrônico de correio, mediante solicitação no endereço <https://www3.ghc.com.br/minhapagina/> sendo que a criação da respectiva conta obedecerá a critérios de necessidade e possibilidade de acordo com os recursos disponíveis;

Todas as mensagens recebidas de origem desconhecida deverão ser eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos. Quaisquer tipos de comunicados e informativos corporativos deverão ser previamente aprovados pelas chefias correspondentes, antes da sua divulgação;

É proibido configurar e/ou manter configuradas contas de correio eletrônico de servidores externos, isto é, diferentes de (@ghc.com.br). **Em caso de dúvidas as solicitações deverão ser encaminhadas à GI;**

O correio eletrônico poderá ser utilizado a partir de qualquer computador conectado à rede do GHC, utilizando-se o sistema GroupWise, ou através da internet, disponível no site do GHC. Este site poderá ser acessado através do endereço <http://www.ghc.com.br>, serviços on line, link para correio eletrônico.

As caixas postais de contas de correio eletrônico do GHC (@ghc.com.br) tem, por padrão, limite de tamanho de 2Gb (2 Gigabytes), salvo condições especiais. Mensagens enviadas/recebidas poderão conter arquivos anexos com até 20MB (20 Megabytes) por mensagem;

O conteúdo das mensagens enviadas através de contas de correio do GHC (@ghc.com.br) é de inteira responsabilidade do usuário que utiliza a conta e

que possui a senha com acesso exclusivo à caixa postal e para envio de mensagens;

É proibida a utilização do e-mail para fins ilegais, transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis;

É proibida a utilização de e-mail para transmitir mensagens conhecidas como Spam, JunkMail, correntes ou a distribuição de mensagens em massa não solicitadas;

III. Recursos de Rede

Todos os recursos de rede de computadores deverão ser utilizados exclusivamente para fins profissionais. Recomendações no controle de acesso:

- Recursos automáticos – Será fornecido aos usuários, mediante autenticação (login), o acesso aos serviços básicos como correio eletrônico, aplicações de produtividade e browser WEB. Estas facilidades básicas irão variar de acordo com os cargos e serão determinadas pela chefia do setor a qual está vinculado. Os recursos dos sistemas são providos via perfis de trabalho ou por uma solicitação especial feita ao proprietário da informação envolvida. A existência de acessos privilegiados, não significa por si só, que um indivíduo esteja autorizado a usar esses privilégios. Se os usuários tiverem quaisquer questões sobre controle de acessos privilegiados, deverão direcionar suas perguntas a Gerência de Informática;
- Solicitação de acesso – As solicitações para novas identificações de usuários devem ser realizadas através do endereço: <https://www3.ghc.com.br/minhapagina>. Alterações de privilégios devem ser feitas por escrito e aprovadas pela chefia imediata do usuário antes que um administrador de sistema realize tal solicitação. As chefias devem declarar, claramente, por que são necessárias alterações nos privilégios de dado colaborador e a relação de tais alterações com as atividades exercidas;
- O processo de aprovação do acesso deve ser iniciado pelo superior do usuário e os privilégios garantidos continuarão em efeito até que o usuário mude suas atividades ou deixe a instituição. Se um desses dois eventos ocorrer, o superior hierárquico tem que notificar imediatamente a Gerência de Informática. Todos aqueles que não são usuários diretos do GHC (contratados, consultores, residentes, temporários, etc) têm que se submeter a um processo semelhante através da gerência a qual está vinculado. Os privilégios destas pessoas deverão ser imediatamente revogados quando da finalização do projeto ou contrato. O mesmo deverá ser observado no desligamento antecipado, considerando ainda a responsabilização pelas atividades e atos cometidos durante a sua permanência na instituição;
- Termo de Responsabilização e Sigilo – Todos os usuários que desejam usar os sistemas do GHC devem aceitar o termo de ciência antes da criação de uma identificação de usuário. O termo está disponível na mesma página de solicitação de acesso – <https://www3.ghc.com.br/minhapagina/> . Nos casos em que o usuário já possua a identificação e acesso, mas que ainda não tenha

oficializado seu consentimento, deverá acessar o link acima . A assinatura deste termo indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos do GHC relacionados ao ambiente de TI (incluindo as instruções contidas neste documento), bem como as implicações legais decorrentes do não cumprimento do disposto no termo;

- Senha de Acesso – As senhas de acesso são controles de segurança essenciais para os sistemas de segurança do ambiente de TI do GHC. Para garantir que os sistemas de segurança façam a parte do trabalho para o qual eles foram desenvolvidos, os usuários devem escolher senhas que sejam difíceis de serem deduzidas;
- Em caso suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas;
- Independente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas para outras pessoas que não o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida;
- Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas. Nestes eventos mecanismos adicionais de segurança serão disparados;
- Todos os arquivos que não tenham fins profissionais devem ser apagados dos equipamentos para evitar problemas futuros com auditorias;
- Todos os computadores do GHC possuem antivírus instalados e são periodicamente atualizados de forma automática. Portanto, é proibido desinstalar e utilizar computadores sem antivírus instalado. Em caso de dúvidas, solicitar orientação a GI;
- É expressamente vedado aos usuários a instalação ou remoção de programas de computador, componentes e periféricos;
- É proibido aos usuários conectar computadores pessoais ou de terceiros à rede corporativa do GHC, exceto com a autorização da GI;
- É proibido realizar conexões Dial-Up, tecnologia 3G, ou outro tipo de conexão, que não os disponíveis nos computadores conectados à rede do GHC, exceto com expressa autorização da GI.

IV. Armazenamento de Arquivos

O GHC dispõe de servidores específicos, com espaço finito para armazenamento de arquivos. Diariamente é executada a rotina de **backup** (cópia de segurança) destes servidores, o que inclui todas as bases de dados e arquivos dos usuários na rede. O **backup** existe para auxiliar na prevenção de perda de dados, como arquivos apagados acidentalmente por falha física ou humana. Isso garante a integridade dos dados, de configurações, bancos de dados e arquivos de usuários.

Cada usuário possui uma unidade de rede (L) com acesso exclusivo para armazenar arquivos. Esta unidade, bem como todas as outras unidades de rede, só deve ser usada para armazenar conteúdo relacionado aos processos de trabalho desempenhados pelo colaborador.

Fica vedado o armazenamento de qualquer mídia de cunho racista, de conteúdo adulto, ofensivo ou protegido por direitos autorais (livros digitais, mp3, fotos particulares, entre outros), seja na rede ou nos discos locais dos computadores. A GI se reserva o direito de apagar tais conteúdos sem prévio aviso.

A Gerência de Informática não realiza backups das unidades locais (C:). Portanto, todos os arquivos importantes devem ser salvos na rede.

V. Internet

Todo o acesso à Internet, através da rede do GHC, é permanentemente monitorado e auditado. O GHC dispõe de softwares de controle de conteúdo, software de reputação das páginas acessadas e antivírus, bem como outros mecanismos de segurança, que permitem uma navegação segura. Quando solicitado pela diretoria, gerentes ou coordenadores das áreas, a Gerência de Informática poderá disponibilizar relatórios com informações como: nomes, datas, páginas consultadas, tempo de consulta, entre outras informações.

Todos os computadores do GHC possuem acesso de nível padrão as páginas da internet. Cada computador poderá ter seu nível alterado, desde que a chefia do setor informe por escrito à Gerência de Informática.

Os usuários são responsáveis por toda a utilização da Internet em computadores da instituição.

É proibido aos usuários configurar ou alterar as configurações de rede e de acesso à Internet dos computadores do GHC, 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 à GI;

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

É proibido o acesso a sites do gênero relacionamento;

Não é permitido o acesso a sites de Internet com conteúdo pornográfico, jogos, batepapo, chat, blogger, cartoon, relacionamento, música, hacker ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança;

É proibido o acesso a sites, a instalação e a utilização de programas de troca de mensagens instantâneas, salvo se comunicado formalmente à Gerência de Informática pela chefia imediata.

A utilização de sites do tipo Proxy é proibida e será considerada falta grave.

Sempre que os usuários, utilizando a Internet, tiverem acesso a materiais criminosos como pornografia infantil (arte, textos, figuras, cenas, imagens) e outros, mesmo que de maneira esporádica e involuntária, deverão entrar em contato imediatamente com a GI.

VI. Rede Sem Fio (WiFi)

O GHC possui uma rede WiFi incipiente, mas extremamente estruturada e segura. Todos os colaboradores que estiverem no raio de cobertura dessa rede, poderão fazer uso dela.

O SSID da rede (nome da rede) disponível aos colaboradores da instituição é GHC_Corp. Para que possam se autenticar a rede, é necessário criar o login em <https://www3.ghc.com.br/minhapagina> na opção Wi-Fi GHC.

Pessoas que se enquadrarem no tipo: acompanhante, estagiário, fornecedor, paciente, terceirizado ou visitante, poderão utilizar a estrutura Wi-Fi do GHC. Para isso, deverão se dirigir a recepção de cada área e efetuar o cadastro. Esses usuários deverão autenticar-se no SSID GHC_Guest, e terão a senha expirada em 6 dias.

Usuários autorizados poderão conectar computadores ou outros equipamentos portáteis e pessoais à Internet, utilizando a rede sem fio “Wi-Fi” do GHC.

O acesso à rede do GHC é um direito concedido a cada usuário, de forma pessoal e intransferível.

Cada usuário é único e total responsável pelo seu código de acesso à rede (login e senha), assim como por todas as ações realizadas por este código.

O usuário terá direito de utilização à rede durante o seu tempo de permanência na instituição.

O GHC compromete-se apenas em prover o acesso à Internet, via rede Wi-Fi, não se responsabilizando por nenhum prejuízo causado por eventual indisponibilidade de sinal ou cobertura, bem como a perda de dados e informações de qualquer natureza.

A manutenção do equipamento e do software contido no mesmo é de total responsabilidade do usuário, não cabendo ao GHC nenhuma responsabilidade referente ao suporte dos mesmos.

A criação e manutenção de cópias de segurança (backup) dos arquivos contidos no(s) equipamento(s) conectado(s) pelo usuário à rede são de inteira responsabilidade do usuário.

O GHC se reserva o direito de cancelar o acesso fornecido a qualquer momento, sem aviso prévio.

Todo o acesso à Internet através da rede Wi-Fi do GHC será controlado pela mesma política de utilização de internet na rede do GHC, e levado em consideração o descrito no Marco Civil da Internet (Lei nº. 12965 de 23 de abril de 2014).

Os usuários são responsáveis por toda a utilização da Internet através da rede WiFi do GHC, e são igualmente passíveis de serem identificados e responsabilizados em caso de acesso indevido.

3.7 Penalidades

A GI alerta todos os usuários que a instalação ou utilização de softwares não autorizados constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa.

Todos os usuários são responsáveis pelo uso correto das ferramentas eletrônicas de propriedade do GHC.

Todas as práticas que representam ameaças à segurança da informação serão tratadas com a aplicação de ações disciplinares. Portanto, na ocorrência de infrações a este Manual, ou às determinações constantes de comunicações externas ou internas, ou mesmo às ordens de superiores hierárquicos, quando for o caso, ficam os infratores sujeitos às seguintes penalidades: advertência verbal, advertência por escrito, suspensão, demissão sem ou com justa causa e/ou outras medidas judiciais cabíveis.

Todos os usuários de informática passam a receber uma cópia deste Manual, dando ciência de seu conteúdo. Os novos colaboradores/usuários receberão o mesmo material por ocasião de sua admissão no GHC.

A GI se reserva o direito de atualizar, alterar, anular toda ou em parte as normas aqui contidas, a qualquer momento e sem aviso. Uma versão atualizada deste manual estará sempre disponível na Intranet do GHC.

4. ATIVIDADES NÃO PERMITIDAS E SUAS RECOMENDAÇÕES

1. Introduzir códigos maliciosos nos sistemas de TI;
2. Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;
3. Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;
4. Tentar interferir desautorizadamente em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;
5. Alterar registro de evento dos sistemas de TI;
6. Modificar cabeçalho de qualquer protocolo de comunicação de dados;
7. Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;
8. Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;

9. Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;
10. Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;
11. Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente;
12. Armazenamento ou uso de jogos em computador;
- 13 . Uso de recurso informacional da entidade pública para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza;
14. Uso de aplicativos não homologados nos recursos informacionais do Órgão Público.