POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. INTRODUÇÃO

A Política de Segurança da Informação ("PSI") tem por objetivo estabelecer regras sobre como todos os ativos de informação, em meio físico e digital, devem ser tratados, atendendo às boas práticas de segurança e à Lei Geral de Proteção de Dados (LGPD).
A Política de Segurança da Informação do Grupo Hospitalar Conceição ("**GHC**") – PSI/GHC visa preservar a confiabilidade, integridade e disponibilidade das informações para a resolução de problemas e tomada de decisão.

2. ALCANCE

Esta Política é aplicável a todas os agentes públicos, titulares e usuários que se relacionem com o "**GHC**", em todas suas unidades de atendimento, em todos os processos que envolvam o tratamento de dados pessoais.

3. COMPOSIÇÃO DA PSI/GHC

A estrutura da PSI/GHC é composta por um conjunto de documentos hierarquicamente descritos a seguir:

- **Política de Segurança da Informação**: constituída por este documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação. A aprovação deste documento é dada pelo Conselho de Administração e sua revisão deverá ser bianual e quando necessário;
- **Normas de Segurança da Informação**: descrevem todas as regras de segurança definidas de acordo com as diretrizes da Política, a serem seguidas em diversas situações em que a informação é tratada. É de responsabilidade do Comitê Gestor da Política e Segurança da Informação do GHC – CGPSI/GHC elaborar o referido documento, bem como revisá-lo periodicamente;
- **Procedimentos de Segurança da Informação**: visam instrumentalizar o disposto nas Normas e na Política. Cabe ao gestor de Tecnologia da Informação elaborar e implantar os procedimentos de segurança adotados, devendo este documento ser revisto bianualmente.

4. ACESSO AO DOCUMENTO

A presente Política e demais documentos a ela associados estarão disponíveis em:

https://www.ghc.com.br/privacidade

5. DIRETRIZES GERAIS

No tratamento de todas as informações do **GHC**, todos agentes públicos, além da legislação e demais políticas e normas adotadas, deverão ter em vista, sobretudo, preservar a:

- Confidencialidade: Garantir que a informação, sempre que necessário, esteja disponível apenas aos agentes públicos vinculados ao **GHC** e nos procedimentos operacionais que a informação esteja sempre protegida do conhecimento de agentes não autorizados;

- Integridade: Garantir a exatidão, integridade, revisão e confidencialidade dos ativos de Informação;
- Disponibilidade: Garantir que os ativos de Informação e recursos de acesso estejam acessíveis sempre que necessário aos agentes públicos vinculados ao **GHC**.

6. ATIVOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

6.1 Todos os ativos de tecnologia da informação e comunicação (ATIC's) do **GHC**, como e-mail, telefone, internet, devem ser utilizados exclusivamente para o desempenho de atividades relacionadas à operação da organização. Jamais poderão ser utilizados para fins indevidos, como:

- Enviar mensagens com ofensas ou que conflitem com os interesses do **GHC**;
- Enviar mensagens com informações do **GHC** a terceiros estranhos à organização, sem que haja justificativa e autorização para tanto;
- Enviar mensagens utilizando assinatura ou endereço falso, com fins de falsificar ou adulterar o conteúdo da mensagem, fazendo-se passar por outra pessoa;
- Enviar mensagens para múltiplos destinatários, salvo nos casos em que o conteúdo do e-mail seja relacionado aos legítimos interesses do **GHC** e mediante prévia autorização do gestor do setor;
- Enviar ameaças eletrônicas como: spam, vírus e outros malwares ou com arquivos com códigos executáveis (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que apresente riscos à segurança;
- Acessar ou tentar acessar conta de outra pessoa sem autorização;
- Acessar ou tentar acessar informações confidenciais sem autorização ou monitorar de forma secreta outros agentes públicos;

6.2 O agente público não deverá abrir links e documentos recebidos de fontes desconhecidas. Caso desconfie de qualquer material recebido, a mensagem não deverá ser aberta e a área de Tecnologia da Informação ou o Comitê Gestor da Política e Segurança da Informação do **GHC** deverá ser comunicado imediatamente.

6.3 É vedada a utilização dos ATICs do **GHC** para acessar, armazenar, divulgar ou propagar qualquer material ligado à pornografia, pedofilia, jogos, racismo, homofobia ou qualquer outro conteúdo ilícito.

6.4 Documentos e softwares desenvolvidos por agentes públicos são de propriedade do **GHC**, ressalvados em casos expressamente regulados por instrumentos contratuais ou não-contratuais por escrito.

6.5 Apenas agentes públicos devidamente autorizados a falar em nome do **GHC** para meios de comunicação ou entidades externas poderão manifestar-se, seja por e-mail, entrevista on-line, documento físico, ligação telefônica.

7. LOGINS E SENHAS

7.1 As credenciais (crachás, logins, senhas e demais credenciais de acesso a ambientes físicos e digitais) são pessoais e intransferíveis e não devem ser compartilhadas com terceiros.

7.2 É obrigação dos agentes públicos manter o sigilo de logins e senhas de acesso aos sistemas do **GHC**, sob pena de incorrer em sanções disciplinares solidariamente com o terceiro com o qual tenha compartilhado suas credenciais; o uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

7.3 As senhas utilizadas em sistemas computacionais do **GHC** deverão ser diversas de senhas particulares.

7.4 Logins e senhas não deverão ser transmitidos por e-mail, chamados ou aplicativos de mensagens (ex. SMS, WhatsApp, Skype, Telegram etc.) e jamais devem ser deixados expostos em qualquer forma de anotação, como agenda, blocos de notas, papéis adesivos, entre outros do tipo.

7.5 É proibido o compartilhamento de login para funções de administração de sistemas.

7.6 As senhas deverão seguir os seguintes pré-requisitos: tamanho mínimo de oito caracteres; existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais; não devem ser baseadas em informações pessoais de fácil dedução.

8. ACESSOS

8.1 A extensão dos acessos concedidos aos agentes públicos será definida de acordo com perfis de acesso, correspondentes à função desempenhada pelo agente público interno ou externo, os quais serão detalhados na matriz de acessos a ser gerida pela área de Tecnologia da Informação.

8.2 Acessos que extrapolam as permissões definidas para o perfil previsto na matriz de acessos serão considerados privilegiados e somente poderão ser concedidos mediante avaliação de necessidade concreta e mediante solicitação do gestor da área.

8.3 A Gerência de Recursos Humanos ou os respectivos gerentes das áreas deverão comunicar, no menor tempo possível, à Gerência de Informática sobre a necessidade de concessão, alteração ou cancelamento de acessos de agentes públicos aos sistemas de informação, de modo que nenhum agente público possua acessos incompatíveis com sua função.

8.4 O agente público não deverá acessar pastas, arquivos, sistemas e qualquer conteúdo que não seja necessário ao desenvolvimento de suas atividades ou após o término de seu relacionamento com o **GHC**. Caso identifique que possui acesso a conteúdo desnecessário, comunique imediatamente à sua gerência ou a Gerência de Informática para que seja realizado o ajuste de seu acesso.

8.5 Após o encerramento de seu relacionamento, nenhum agente público, titular ou usuário, deverá manter qualquer tipo de acesso aos ativos de informação do **GHC**, devendo cessar imediatamente o uso das credenciais às quais tinha acesso durante o relacionamento contratual.

8.6 Dados pessoais referentes à saúde de agentes públicos serão acessados exclusivamente pela Gerência de Recursos Humanos. Quando necessário, a Gerência de Recursos Humanos informará os reflexos de tais informações aos gestores competentes, sem, contudo, revelar os detalhes dos dados em si.

8.7 A concessão de acesso à rede sem fio para acesso apenas à internet se dará através de cadastro feito na Gerência de Informática junto com equipe de rede. Ficam estabelecidos os seguintes períodos de acesso: 1 (um) ano para agente públicos, 6 (seis) meses para estudantes e 1 (uma) semana para usuários/titulares.

9 SEGURANÇA NAS ESTAÇÕES DE TRABALHO

9.1 Ao se ausentar de sua mesa o agente público deverá bloquear a tela ou guardar os dispositivos, bem como guardar todos os documentos que não for levar consigo, preferencialmente em sua gaveta ou armário, trancando e levando a chave, de modo que não seja possível a outras pessoas visualizarem informações expostas na estação de trabalho e/ou em seu monitor.

9.2 Documentos físicos devem ser armazenados de forma segura, em arquivo próprio com acesso restrito, não devendo ser deixados em exposição na estação de trabalho ou outros ambientes na ausência do agente público.

9.3 Arquivos digitais devem ser armazenados na rede interna do GHC ou em outros locais adequados, não devendo ser salvos no próprio computador do agente público, em sua área de trabalho.

9.4 O agente público deve evitar a impressão de documentos ou informações, dando preferência para a leitura diretamente nas telas dos dispositivos. Caso seja necessária a impressão, o documento deverá ser coletado imediatamente na impressora.

9.5 Os armários, gavetas ou arquivos, devem sempre permanecer fechados e as chaves nunca deverão ser deixadas na fechadura.

9.6 Ao término do expediente os ambientes devem ser trancados com chave, a qual ficará sob responsabilidade do gestor da área ou de quem ele determinar.

9.7 Informações confidenciais do **GHC** não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel etc.) sem as devidas autorizações e proteções.

9.8 Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais).

9.9 Somente softwares homologados pelo **GHC** podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia da Informação.

9.10 Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio.

9.11 É vedada a abertura de computadores para qualquer tipo de reparo pelos agentes públicos. Caso seja necessário, o reparo deverá ser feito pela equipe da Gerência de Informática.

9.12 Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede interna do **GHC** mediante autorização do chefe imediato via memorando e prévio cadastro e liberação do setor de Tecnologia da Informação.

9.13 É proibida a impressão de documentos de cunho pessoal e/ou ilegal.

9.14 A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica da Gerência de Informática.

9.15 O gestor de cada gerência ou de cada setor será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões excessivas;

9.16 As impressoras devem estar ligadas na energia através dos seus transformadores e serão proibidas intervenções desta natureza por parte de qualquer agente público que não seja do setor de Gerência de Informática.

10 BACKUP

10.1 Os arquivos inerentes ao **GHC**, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais.

10.2 Todo sistema ou informação relevante para a operação dos negócios do **GHC** deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição.

10.3 As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e provocar o SGPTI sobre a necessidade de backup deles, sugerindo o tempo de retenção destas cópias.

10.4 Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de agentes públicos vinculados ao **GHC** ou processos aos sistemas de informática.

10.5 As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do datacenter.

10.6 Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento.

10.7 Na situação de erro de backup e/ou restauração é necessário que seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse *backup*, eles deverão ser executados apenas mediante justificativa de necessidade.

11 MONITORAMENTO E SEGURANÇA

11.1 Todos os agentes públicos devem ter ciência de que o uso dos ativos de tecnologia da informação e comunicação, especialmente a internet, podem ser monitorados e os registros obtidos podem servir de evidência para fins jurídicos e aplicação de medidas disciplinares.

11.2 Neste sentido, com o único fim de assegurar o cumprimento das diretrizes presentes nesta PSI, o **GHC** poderá:

- Monitorar os ativos de informação e analisar o uso deles. A informação gerada por esses sistemas poderá ser usada para identificar agentes públicos e respectivos acessos efetuados, bem como material manipulado;
- Realizar, sem aviso prévio, a qualquer tempo a inspeção física ou auditoria nos ativos de seu uso;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

12 CLASSIFICAÇÃO DA INFORMAÇÃO

12.1 As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

- Pública: São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico. São exemplos de

informação pública: editais de licitação; rotinas e agendas médicas; campanhas de promoção à saúde;

- Institucional: Qualquer informação que circule internamente cujo acesso dos agentes públicos é livre.
- Confidencial: Qualquer informação que contém dados estratégicos e sigilosos, cujo acesso deve ser controlado.

13 INCIDENTES DE SEGURANÇA

13.1 Um incidente é qualquer evento que resulte ou que tenha possibilidade de resultar em perdas ou danos às informações e dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento de ativos.

13.2 Caso identifique algum incidente, o agente público deverá no prazo máximo de 24 horas, comunicar a Gerência de Informática ou ao Encarregado pelo Tratamento de Dados, pelo canal de comunicação de incidentes.

13.3 A comunicação deverá conter data, hora, local, possíveis causas, ativos comprometidos, dentre outros que o que o agente público julgar necessário;

13.4 No tratamento de incidentes a área de Tecnologia da Informação ou o Encarregado pelo Tratamento de Dados tratará a ameaça, risco ou incidente por meio dos seguintes passos:

- Elaborar relatório contendo o máximo de informações possível, como descrição do ocorrido, áreas afetadas, possíveis causas, natureza, categoria e quantidade de dados pessoais ou sistemas afetados, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis para os titulares e para o GHC;
- Proceder com adoção de medidas, isolamento de danos, caso seja necessário paralisar áreas e sistemas comprometidos;
- Em se tratando de efetivo incidente e verificados riscos ou danos relevantes aos Titulares de dados, a comunicação aos Titulares e à ANPD será realizada, necessariamente, com apoio do Comitê Gestor da Política e Segurança da Informação do GHC, que avaliará a forma mais adequada de abordagem das pessoas afetadas, podendo contar com agentes internos ou externos de marketing;
- Após aprovação do Comitê Gestor da Política e Segurança da Informação do GHC e da Diretoria, o Encarregado emitirá comunicado à ANPD e aos Titulares afetados no prazo de 2 (dois) dias úteis contados da verificação do incidente ou em outro prazo fixado em regulamentação específica pela ANPD. A comunicação à ANPD será realizada utilizando-se o formulário específico disponível no site da autoridade e por meio do sistema de peticionamento eletrônico;
- Evidenciar e comprovar as possíveis causas da ameaça, risco ou incidente;
- Realizar o tratamento em si da ameaça, risco ou incidente, analisando todas as possíveis soluções para resolução;

- Garantir que não haja outras ameaças, riscos ou incidente relacionados ao caso descrito na comunicação;
- Realizado o tratamento com a adoção de todas as medidas técnicas e administrativas remeter ao Comitê Gestor da Política e Segurança da Informação do GHC para a validação.

14 COMUNICAÇÃO

Sempre que se deparar com um risco ou efetiva violação de segurança aos ambientes de informação físicos e digitais do **GHC**, o agente público, deverá comunicar pelo e-mail dpo@ghc.com.br ou diretamente ao seu gestor imediato, reportando o maior número possível de informações sobre o fato.

15 TREINAMENTOS

O Comitê Gestor da Política e Segurança da Informação do **GHC**, dentro de suas responsabilidades, deverá promover a todos os agentes públicos vinculados ao **GHC** que utilizam ativos de informação do **GHC**, de forma periódica, eventos, treinamentos, workshops e demais medidas educativas.

16 SANÇÕES

16.1 As violações ou infrações, ainda que por omissão ou mera tentativa não consumada, desta Política e toda e qualquer diretriz ou norma publicada e veiculada pelo **GHC** poderão ensejar a aplicação de penalidades previstas no Regulamento de Pessoal do GHC.

16.2 As violações que impliquem em atividades ilegais, ou que possam incorrer em riscos aos titulares de Dados Pessoais, ou dano ao GHC, ensejarão a responsabilidade pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

A presente Política de Segurança da Informação do GHC entra em vigor nesta data, em decorrência da sua aprovação pelo Conselho de Administração do Grupo Hospitalar Conceição.

Porto Alegre, 05 de maio de 2022.