



Manual da Política de Segurança da Informação

2ª Versão 2025

Prezados (as),

É com grande satisfação que a Diretoria-Executiva do GHC apresenta aos agentes públicos do GHC o Manual da Política de Segurança da informação da nossa estatal.

A Política de Segurança da Informação foi elaborada em conformidade com a Resolução CGPAR/ME nº41/2022, alinhada as boas práticas de governança de Tecnologia de Informação e a Lei Geral de Proteção de Dados – LGPD.

O objetivo desta política é estabelecer regras sobre como todos os ativos de informação, em meio físico e digital, devem ser tratados.

Boa Leitura!

Você sabe o que é segurança da informação?

É o conjunto de medidas e práticas adotadas para proteger as informações de uma organização, garantindo sua confidencialidade, integridade e disponibilidade.

Por que a segurança da informação é importante?

É fundamental para preservar a confiabilidade, integridade e disponibilidade das informações para a resolução de problemas e tomada de decisão, além de prevenir o acesso indevido ou uso mal-intencionado de informações sensíveis.

Qual abrangência da Política de Segurança da Informação?

Essa Política se estende a todos os agentes públicos, titulares e usuários que se relacionem com o GHC, em todas as suas unidades de atendimento, em todos os processos que envolvam o tratamento de dados pessoais.

Quais as diretrizes da Política de Segurança da Informação do GHC?

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.

Como são classificadas as informações?

As informações devem ser classificadas e identificadas por rótulos: **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.

Como devem ser utilizados os ativos de tecnologia da informação e comunicação (ATIC's) do GHC, como e-mail, telefone e internet?

As ATIC's do GHC, tais como e-mail, telefone e internet, devem ser utilizados somente para as atividades relacionadas à organização. Eles não devem ser usados para enviar mensagens ofensivas ou em conflito com os interesses do GHC, fornecer informações a pessoas não autorizadas, fazer-se passar por outra pessoa ou enviar ameaças eletrônicas. Além disso, o agente público não deve acessar informações confidenciais sem autorização, abrir documentos ou links de fontes desconhecidas e propagar materiais ilícitos, como pornografia e racismo. Finalmente, somente agentes públicos autorizados podem falar em nome do GHC para meios de comunicação ou entidades externas.

Quais são as orientações para o uso de logins e senhas em sistemas do GHC?

As credenciais são pessoais e intransferíveis, e não devem ser compartilhadas. É obrigação dos agentes públicos manter o sigilo de suas credenciais e o uso de dispositivos e/ou senhas de identificação de outra pessoa é crime. As senhas utilizadas devem ser diferentes das senhas particulares e seguir pré-requisitos como um tamanho mínimo de oito caracteres, caracteres pertencentes a pelo menos três grupos, e não devem ser baseadas em informações pessoais. Logins e senhas não devem ser compartilhados para funções de administração de sistemas e não devem ser transmitidos por e-mail, chamados ou aplicativos de mensagens, e nem devem ser deixados expostos em qualquer forma de anotação.

Qual é a Política de Segurança da Informação em relação aos acessos de agentes públicos aos sistemas de informação do GHC?

Define que os acessos dos agentes públicos serão concedidos de acordo com perfis de acesso correspondentes às funções que desempenham, com permissões definidas na matriz de acessos. A concessão de acessos privilegiados só será feita após avaliação da necessidade e solicitação do gestor da área. A Gerência de Recursos Humanos ou as gerências das áreas devem comunicar alterações ou cancelamentos de acessos. O agente público não deve acessar conteúdos desnecessários. Após o encerramento de seu relacionamento, deve cessar imediatamente o uso das credenciais de acesso. A concessão de acesso à rede sem fio será feita através de cadastro junto à equipe de rede.

Como é realizada a Política de Segurança da Informação nas estações de trabalho do GHC?

- 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.
- 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.
- 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.
- 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.
- Os armários, gavetas ou arquivos, devem sempre permanecer fechados e as chaves nunca deverão ser deixadas na fechadura.
- 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.
- Informações confidenciais do GHC não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel etc.) sem as devidas autorizações e proteções.
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais).
- 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.
- Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio.
- 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.
- 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.
- É proibida a impressão de documentos de cunho pessoal e/ou ilegal.

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

Qual é a política do GHC para garantir a segurança no armazenamento e backup de dados?

A Política de Segurança da Informação do GHC estabelece que os arquivos do sistema devem ser armazenados na pasta compartilhada de cada setor, não em equipamentos pessoais. É necessário ter cópias de backup de dados relevantes para minimizar impactos nas operações em caso de ocorrer algum incidente. As áreas de negócio devem classificar os dados conforme a relevância e solicitar backup ao setor responsável. Os backups devem ser automatizados e realizados fora do horário comercial. As mídias de backup devem ser armazenadas em local seguro e distante do datacenter. A infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança e os problemas devem ser solucionados rapidamente. Se necessário, o backup pode ser adiado mediante justificativa.

Quais são as medidas de proteção de dados que os agentes públicos precisam tomar de acordo com as diretrizes da Política de Segurança da Informação?

Os agentes públicos devem estar cientes de que o uso de tecnologias da informação e comunicação, como a internet, podem ser monitorados e seus registros usados como evidência jurídica ou disciplinar. Com o objetivo de garantir o cumprimento das diretrizes da Política de Segurança da informação, o GHC pode monitorar e analisar o uso dos ativos de informação, realizar inspeções físicas e auditorias sem aviso prévio, e instalar sistemas de proteção para a segurança das informações e dos acessos.

Qual é o procedimento para lidar com um incidente de segurança no âmbito público, de acordo com a política de segurança da informação do GHC?

A política de segurança da informação prevê que qualquer incidente que possa resultar em perdas ou danos às informações e dados pessoais deve ser comunicado à Gerência de Informática ou ao Encarregado pelo Tratamento de Dados em até 24

horas. O tratamento do incidente envolve a elaboração de um relatório, adoção de medidas para isolar danos e, se for caso, paralisar áreas e sistemas comprometidos. Quando há riscos relevantes aos titulares de dados, a Autoridade Nacional de proteção de Dados (ANPD) e os titulares devem ser comunicados com a ajuda do Comitê Gestor da Política e Segurança da Informação do GHC. Por fim, todas as possíveis soluções para resolução devem ser analisadas, e após a adoção das medidas técnicas e administrativas, será feita uma validação pelo Comitê Gestor.

O que fazer em caso de suspeita de violação da segurança da informação?

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.

Quais as consequências caso eu infrinja a Política de Segurança da Informação?

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. 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

Você sabe onde acessar o documento na íntegra?

A presente política e demais documentos a ela associados estarão disponíveis em: <https://www.ghc.com.br/privacidade>.