

---

**Título:** POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO HCOR

---

**Versão do documento:** V.2

---

**Elaborado por:** Gerência de Segurança da Informação

---

## 1. Objetivos

Estabelecer diretrizes que possibilitem os colaboradores, terceiros e parceiros do Hcor seguirem padrões de comportamento desejáveis e aceitáveis de acordo com a legalidade e boas práticas mundiais de Segurança da Informação, resguardando o Hcor quanto à confidencialidade, integridade e disponibilidade das informações e mitigando os riscos ou qualquer outro impacto negativo, que seja resultado de uma falha de segurança.

## 2. Abrangência

Complexo Paraíso  
Unidade Avançada Cidade Jardim

## 3. Definições

**Ativo:** Bens do Hcor que têm valor econômico, incluída a informação e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

**Colaboradores:** Funcionários, temporários, menores aprendizes, estagiários e prestadores de serviços.

**Incidente de segurança da informação:** um evento isolado, ou uma série de eventos relacionados à segurança da informação que são indesejados ou inesperados e podem comprometer as operações de negócios, ameaçando a segurança da informação.

**Informação:** todo e qualquer conteúdo ou dado que tenha valor para a organização.

**Segurança da Informação:** preservação do sigilo, da integridade e da disponibilidade de informações.

## 4. Descrição

### 4.1 Diretrizes da política de Segurança da Informação

- a) As informações do Hcor e dos clientes são sigilosas e devem ser tratadas de forma ética de acordo com as políticas internas, evitando-se mau uso e exposição indevida;
- b) As informações relacionadas ao cuidado aos pacientes são de caráter estritamente sigilosos e devem estar disponíveis apenas no sistema utilizado



como prontuário, e apenas aos profissionais relacionados à sua assistência e ao próprio paciente.

- c) A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação indispensáveis para o desempenhar suas atividades e por autorização dos superiores hierárquicos aos mesmos;
- d) A senha é utilizada como assinatura eletrônica, deve ser mantida em sigilo absoluto e não deve ser compartilhada;
- e) Quaisquer relações com prestadores de serviços devem existir com base em contratos das atividades correspondentes. Todos os profissionais que atuam no Hcor devem seguir seus respectivos códigos de ética e/ou termos de confidencialidade de informações a qual tenham acesso;
- f) A utilização de informações do Hcor e seus pacientes por meio das redes sociais é monitorada pela área de marketing, e devem seguir as diretrizes descritas no Guia de Boas Práticas nas Redes Sociais. Outras informações relacionadas ao Hcor, só serão publicadas caso haja autorização pelas lideranças da organização.

## **4.2 Tratamento da informação e proteção de dados pessoais**

Todo tratamento de dados pessoais realizado no Hcor deverá respeitar a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e outras normas sobre a matéria, incluindo regulações publicadas pela Autoridade Nacional de Proteção de Dados, assim como seguir as diretrizes da política interna de proteção de dados.

## **4.3 Sistema de gestão de Segurança da Informação (SGSI)**

O Sistema de Gestão de Segurança da Informação (SGSI) consiste nas políticas, procedimentos, diretrizes, recursos e atividades, com o objetivo de proteger os ativos de informação. O sistema é uma abordagem sistemática para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a Segurança da Informação do Hcor para alcançar os objetivos de negócios.

## **4.4 Gestão de Segurança da informação**

Para manter um nível satisfatório de segurança das informações, o Hcor constituiu a equipe de Segurança da Informação e adota as seguintes diretrizes:

- a) O controle de acesso dos colaboradores aos ativos de informação deve ser aprovado pela equipe de Segurança da Informação. Os acessos devem ser rastreáveis.
- b) O acesso físico nos Data Centers e Salas de Telecom dos colaboradores e terceiros devem ser registrados.
- c) Cópias de segurança devem ser testadas e consideradas vitais para o sistema e para a retomada das atividades da área em caso de



contingência;

- d) Em caso de desastres, alternativas de recuperação devem ser seguidas de acordo com o dano ao ambiente, minimizando interrupções nas operações e possibilitando a continuidade dos processos de negócios.
- e) A utilização da internet nos computadores do Hcor deve ser prioritariamente para os negócios.
- f) Regras para a aquisição e desenvolvimento de sistemas devem ser estabelecidas e aplicadas.
- g) As redes devem ser identificadas, segregadas e monitoradas;
- h) Dispositivos móveis do Hcor destinam-se ao uso em serviço para realização de suas atividades de trabalho, devendo ser utilizado somente para esta finalidade. A concessão de acesso remoto deve ser autorizada formalmente e solicitada à equipe de Segurança da informação.
- i) As informações devem ser classificadas e manuseadas de acordo com a confidencialidade e as proteções necessárias;
- j) Os ativos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos;
- k) Um processo de gestão de mudança deve estar em vigor, a fim de não ocasionar falhas operacionais ou de segurança no ambiente produtivo do Hcor.
- l) Medidas de segurança são adotadas para garantir a proteção das informações e riscos de acessos não autorizados.
- m) Todos os incidentes que afetam a segurança da informação devem ser reportados à equipe de Segurança da informação através do e-mail de incidentes divulgado internamente.
- n) Um processo de gestão de riscos deve ser seguido.
- o) Para aquisição de produtos e serviços de Tecnologia da Informação e Comunicação devem ser consideradas avaliação e qualificação de segurança da informação dos fornecedores.
- p) Descarte e doações dos equipamentos eletrônicos e mídias de armazenamento devem garantir os requisitos de Segurança da Informação.
- q) Diretrizes de identificação e liberação de acesso físico às dependências do Hcor são determinadas conforme diretrizes da Segurança Patrimonial;
- r) Uso seguro de plataforma de Inteligência Artificial deve ser realizado conforme diretrizes estabelecidas em política do tema;
- s) A utilização de plataformas de Telessaúde devem ser utilizadas de forma responsável e ética, garantindo um processo seguro e de qualidade.

#### 4.5 Comunicação

O conjunto de ações de comunicação foi definido conforme Plano de Comunicação de Segurança da Informação.



Comunicados ou campanhas institucionais serão enviados conforme diretrizes do Marketing.

## **4.6 Das responsabilidades específicas**

### **4.6.1 Dos colaboradores**

Todos os colaboradores do Hcor, serão responsáveis em cumprir e zelar pela realização eficaz das políticas e princípios da Segurança da Informação, no compromisso com os critérios legais e éticos que envolvem o Hcor. É de total responsabilidade de cada colaborador qualquer prejuízo ou dano que vierem a sofrer ou causarem ao Hcor e/ou a terceiros, em decorrência do não atendimento às diretrizes das políticas do Hcor aqui referidas.

### **4.6.2 Dos gestores**

É responsabilidade de cada gestor registrar, atribuir valor, analisar quanto aos riscos e classificar, as informações da sua área. Além de garantir a implementação de mecanismos necessários para descarte seguro das informações.

É de responsabilidade do gestor cumprir e fazer cumprir esta política e demais itens aqui referenciados.

### **4.6.3 Dos prestadores de serviço**

Os prestadores de serviço do Hcor, serão responsáveis em cumprir as políticas e princípios da Segurança da Informação, no compromisso com os critérios legais e éticos que envolvem o Hcor.

### **4.6.4 Dos proprietários de ativos de informação**

O proprietário da informação pode ser um diretor, gerente ou coordenador de uma determinada área ou projeto. É o responsável pela manutenção, revisão e cancelamento de autorização à determinada informação ou conjunto de informações sob sua guarda.

### **4.6.5 Do departamento de Inteligência Digital**

O departamento é responsável por gerir o uso de tecnologias necessárias ao bom andamento do negócio, incluindo ações preventivas e tratamento de incidentes com o propósito de promover maior nível de Segurança da Informação. Além de propor metodologias, processos específicos para a Segurança da Informação, e apoiar iniciativas que visem à segurança dos ativos de informação.

### **4.6.6 Do departamento de Administração de Pessoal, Gestão de Terceiros e Credenciamento Médico**



Formalizar nos contratos individuais de trabalho, a responsabilidade quanto ao cumprimento da política de Segurança da Informação, e comunicar à área de Inteligência Digital formalmente toda e qualquer alteração no quadro funcional da instituição, a fim de evitar acessos não autorizados e/ou desnecessários.

#### **4.6.7 Do departamento Jurídico**

Cabe ao departamento Jurídico acompanhar incidentes que violem significativamente as políticas de Segurança da Informação, além de revisar e sugerir adaptações das documentações citadas, de acordo com as necessidades e perfil de incidentes. Todos os documentos jurídicos relacionados à Segurança da Informação e regulamentações internas, deverão ser revisados pela área para que esteja em conformidade com legislação pertinente à sua área de atuação.

#### **4.7 Auditoria e Monitoramento**

O Hcor deve monitorar e registrar todo o uso de informações geradas e armazenada em nosso ambiente, mantendo controles apropriados e trilhas de auditorias em pontos que julgar como necessário para reduzir riscos. Para isso o Hcor reserva-se no direito de implantar sistemas de monitoramento e acesso às estações de trabalho, servidores internos e externos, e outros componentes da rede. Além de instalar câmeras nas instalações físicas e instalações de sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;

#### **4.8 Descumprimento**

Os colaboradores, terceiros e parceiros são obrigados a seguir os procedimentos descritos nesta política.

Os indivíduos que forem encontrados em descumprimento desta política estão sujeitos a ações disciplinares cabíveis, incluindo advertência, suspensão, demissão por justa causa ou rescisão contratual, sem prejuízo da comunicação às autoridades competentes.

#### **4.9 PERIODICIDADE**

A revisão ou atualização desta política será realizada periodicamente de acordo com a Política de Gestão de Documentos, ou quando a equipe de Segurança da Informação julgar necessário.

## **5. Observações**

### **5.1 Divulgação da política de Segurança da Informação**

A política de Segurança da informação deve ser de conhecimento de todas as partes interessadas. Estes, devem aderir a esta política, comprometendo-se a agir de acordo com as informações da mesma.



## 6. Referências Bibliográficas

### 6.1 Esta política utilizou como referência:

ABNT NBR ISO/IEC 27001:2022;  
ABNT NBR ISO/IEC 27002:2022;  
Manual JCI 7ª edição: 2021;

## 7. Controle de versão

Versão	Descrição da alteração	Data
1	Criação de PSI na versão resumida	11/2023
2	Inclusão de tópicos sobre Telessaúde e Inteligência Artificial, controle de versões e aprovadores	02/2025

---

**Documento na íntegra aprovado em:** 18/12/2024

**Aprovado por:**

Data Protection Officer  
Superintendente de Inteligência Digital  
CEO

---

