



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

Nosso compromisso é **proteger** nossas informações com **ética**, **responsabilidade** e **diligência**, garantindo a **confiança** e a **continuidade** dos nossos negócios.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Diretrizes para **proteger** nossas informações, preservar a **confidencialidade**, a **integridade** e a **disponibilidade** dos dados, garantir a **continuidade** dos nossos negócios e gerar **valor sustentável**.



Integridade em cada escolha,
confiança em cada relacionamento.



SUMÁRIO

Conheça os principais temas desta Política de **Segurança da Informação**.

As diretrizes desta Política orientam a proteção das informações, dos ativos tecnológicos e dos dados tratados pela **Hub Health**, promovendo uma cultura de segurança, responsabilidade e conformidade.

01 Fundamentos

-  **01.** Nosso Compromisso com a Segurança da Informação
-  **02.** Objetivo e Abrangência
-  **03.** O que é Segurança da Informação?

02 Proteção da Informação

-  **04.** Uso Seguro dos Recursos Tecnológicos
-  **05.** Correio Eletrônico e Internet
-  **06.** Controle de Acessos e Senhas
-  **07.** Classificação das Informações
-  **08.** Armazenamento, Backup e Continuidade

03 Governança e Integridade

-  **09.** Uso Responsável da Inteligência Artificial
-  **10.** Incidentes de Segurança da Informação
-  **11.** Papéis e Responsabilidades
-  **12.** Canal de Denúncias
-  **13.** Consequências e Medidas Disciplinares
-  **14.** Nossa Pergunta de Ouro



Integridade em cada escolha,
confiança em cada relacionamento.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

01.

Nosso Compromisso com a Segurança da Informação

A **proteção das informações** é essencial para a confiança que construímos todos os dias com nossos clientes, parceiros, colaboradores e a sociedade.

Por isso, assumimos o compromisso de preservar a **confidencialidade, integridade, disponibilidade** e **autenticidade** das informações, garantindo que sejam utilizadas de forma ética, segura e responsável.

Cada um de nós é **responsável** por proteger os dados e ativos de informação da **Hub Health**, contribuindo para a continuidade dos negócios e para a geração de valor sustentável.



Informação protegida é confiança preservada.
Segurança da informação é compromisso de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

A Segurança da Informação protege o que sustenta nossos negócios

A informação é um dos **ativos mais valiosos** da Hub Health. Sua proteção é essencial para garantir a continuidade das operações, preservar a confiança de clientes, parceiros e colaboradores e assegurar o cumprimento das obrigações legais e regulatórias.

Esta Política estabelece as diretrizes para a proteção das informações corporativas, promovendo uma cultura de segurança baseada em **responsabilidade, prevenção de riscos e conformidade**, alinhada às melhores práticas de governança e aos princípios da **Confidencialidade, Integridade e Disponibilidade (CID)**.



Proteger a informação é proteger a confiança, a reputação e a continuidade dos nossos negócios.

A segurança da informação é responsabilidade de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

02. Objetivo e Abrangência

Esta Política tem como objetivo estabelecer diretrizes para a proteção das informações e dos ativos de informação da **Hub Health**, garantindo a **confidencialidade, integridade, disponibilidade, autenticidade** e rastreabilidade dos dados.



As diretrizes desta Política **aplicam-se a todos** que, de alguma forma, acessam, utilizam, processam ou compartilham informações em nome da **Hub Health**.

Esta Política se aplica a **todos** que se relacionam com a Hub Health, incluindo, mas não se limitando a:



Colaboradores



Diretores



Prestadores
de Serviços



Consultores



Fornecedores



Parceiros de
Negócios



Terceiros atuando
em nome da empresa



Nossa informação é um ativo valioso.
Proteger é um compromisso de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

03. O que é Segurança da Informação?

Segurança da Informação é o conjunto de práticas, processos e tecnologias que protegem as informações e os ativos de informação da **Hub Health** contra acessos não autorizados, alterações indevidas, perdas ou indisponibilidades.

Ela se baseia em **princípios fundamentais** que garantem a proteção dos dados em todas as situações.



A proteção da informação é o que mantém nossa confiança, nossa reputação e a continuidade dos nossos negócios.

Segurança da informação é responsabilidade de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

04.

Uso Seguro dos Recursos Tecnológicos

Os recursos tecnológicos são ferramentas essenciais para o desempenho das nossas atividades e para a proteção das informações.

Cada um de nós é **responsável por utilizá-los de forma segura**, consciente e em conformidade com as políticas da **Hub Health**.

Adote estas práticas no seu dia a dia:



Utilizar apenas equipamentos autorizados

Use somente dispositivos fornecidos ou aprovados pela empresa.



Manter softwares atualizados

Atualizações corrigem falhas e protegem contra ameaças conhecidas.



Bloquear a estação ao se ausentar

Proteja suas informações e impeça o acesso não autorizado.



Utilizar antivírus corporativo

O antivírus corporativo é essencial para a proteção dos nossos sistemas.



Reportar incidentes imediatamente

Comunique qualquer suspeita ou incidente de segurança sem demora.



Respeitar as políticas internas

Siga todas as políticas e procedimentos de segurança da informação.



Pequenas atitudes no uso da tecnologia fazem grande diferença na proteção dos nossos dados.
Segurança da informação é responsabilidade de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

05. Correio Eletrônico e Internet

O correio eletrônico e o acesso à internet são ferramentas importantes para a **comunicação** e realização das atividades profissionais.

Seu uso deve ser feito de forma **consciente, segura e responsável**, sempre em conformidade com as políticas da **Hub Health**.



Utilize com responsabilidade.
Proteja as informações.
Preserve a reputação da empresa.



É PERMITIDO



ATIVIDADES PROFISSIONAIS

Utilize o e-mail e a internet para atividades relacionadas ao trabalho.



ACESSO SEGURO

Acesse apenas sites confiáveis e verifique sempre a segurança das conexões.



COMUNICAÇÃO CORPORATIVA

Utilize o e-mail corporativo para comunicações de trabalho e relacionamento com clientes, fornecedores e parceiros.



É PROIBIDO



PHISHING

Não clique em links suspeitos ou forneça informações confidenciais.



DOWNLOADS ILEGAIS

Não realize downloads de conteúdo protegido por direitos autorais.



SOFTWARES NÃO AUTORIZADOS

Não instale nem utilize softwares não autorizados pela empresa.



USO INADEQUADO DO E-MAIL

Não utilize o e-mail corporativo para assuntos pessoais, correntes, ofensivos, discriminatórios ou que possam comprometer a imagem da empresa.



O uso consciente do e-mail e da internet protege você, seus colegas e a reputação da Hub Health.
Segurança da informação é responsabilidade de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

06. Controle de Acessos e Senhas

O controle de acessos garante que as informações sejam acessadas apenas por pessoas autorizadas e na medida necessária para o desempenho das suas atividades.

Cada colaborador é responsável por proteger suas credenciais e utilizar os recursos da **Hub Health** de forma ética e segura.

SIGA AS ETAPAS PARA UM CONTROLE DE ACESSOS EFICAZ



Acesso consciente hoje, informações protegidas sempre.
Segurança da informação é responsabilidade de todos.



PROTEJA SUAS CREDENCIAIS. PROTEJA A EMPRESA.

Credenciais são pessoais, intransferíveis e inegociáveis.
Em caso de suspeita de uso indevido ou comprometimento, altere sua senha e comunique imediatamente o TI e o Jurídico & Compliance.



Controle de acessos é proteção de informações, proteção de pessoas e proteção do nosso negócio.
Segurança da informação é responsabilidade de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

07.

Classificação das Informações

As informações da **Hub Health** devem ser classificadas de acordo com o seu **nível de sensibilidade**, garantindo o tratamento adequado e a proteção necessária.



Classificar corretamente é **proteger** o que é valioso para a empresa, para nossos clientes e para todos nós.

UTILIZE A CLASSIFICAÇÃO CORRETA E SIGA AS REGRAS DE PROTEÇÃO PARA CADA NÍVEL.



PÚBLICA

Informações de amplo conhecimento.

EXEMPLOS

- ✓ Informações divulgadas no site institucional
- ✓ Materiais de marketing e institucionais
- ✓ Notícias e comunicados públicos
- ✓ Informações disponíveis em fontes abertas



Não requer restrições especiais de acesso.



USO INTERNO

Informações para uso exclusivo da empresa.

EXEMPLOS

- ✓ Políticas e procedimentos internos
- ✓ Apresentações e relatórios internos
- ✓ Documentos administrativos
- ✓ Dados operacionais do dia a dia



Compartilhe apenas com colaboradores que tenham necessidade de acesso.



CONFIDENCIAL

Informações sensíveis e estratégicas.

EXEMPLOS

- ✓ Estratégias de negócio e planos corporativos
- ✓ Informações financeiras não divulgadas
- ✓ Dados de clientes, fornecedores e parceiros
- ✓ Projetos, pesquisas e desenvolvimentos



Acesso restrito a pessoas autorizadas e com real necessidade.



RESTRITA

Informações críticas cujo acesso não autorizado pode causar danos graves.

EXEMPLOS

- ✓ Dados pessoais sensíveis (LGPD)
- ✓ Credenciais, senhas e certificados
- ✓ Informações jurídicas e contratuais sensíveis
- ✓ Dados financeiros sigilosos e não públicos



Acesso extremamente restrito. Exige autorização formal e medidas adicionais de proteção.



EM CASO DE DÚVIDA SOBRE A CLASSIFICAÇÃO, consulte o Jurídico & Compliance.



A PROTEÇÃO DA INFORMAÇÃO É **RESPONSABILIDADE** DE TODOS.



Informação bem classificada é informação bem protegida. Segurança da informação é **responsabilidade** de todos.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

08.

Armazenamento, Backup e Continuidade

Garantimos o ciclo completo de gestão da informação, assegurando que os dados sejam produzidos, armazenados, protegidos por backups, recuperados quando necessário e descartados de forma segura e responsável.



Informação protegida, negócio protegido.

Boas práticas asseguram a disponibilidade, integridade e confidencialidade das informações em todas as etapas do ciclo.



FLUXO



A informação deve estar disponível quando necessária.
Protegemos nossos dados com **armazenamento seguro, backup e continuidade** dos negócios.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

09.

USO RESPONSÁVEL DA INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial é uma ferramenta poderosa que pode impulsionar nossa produtividade e inovação. Seu uso deve ser sempre ético, seguro e alinhado aos valores e às políticas da **Hub Health**.



Uso consciente. Decisões responsáveis.

A IA complementa nossa inteligência, mas não substitui nosso julgamento, nossa ética e nossa responsabilidade.



PERMITIDO

- ✓ Apoio à pesquisa
- ✓ Apoio à redação
- ✓ Automação de tarefas
- ✓ Análise de documentos



Sempre com revisão humana.



PROIBIDO

- ✗ Inserir dados pessoais em IA pública
- ✗ Inserir informações confidenciais
- ✗ Compartilhar estratégias comerciais
- ✗ Utilizar IA para burlar controles
- ✗ Utilizar IA para criar documentos falsos
- ✗ Utilizar IA sem validação humana



O uso da Inteligência Artificial exige responsabilidade.
Agimos com **ética, supervisão humana e proteção das informações**.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

10.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Incidentes podem acontecer.
O que faz a diferença é como reagimos.
Todos têm papel importante para
proteger nossas informações, nossos
clientes e a continuidade do negócio.



Segurança é responsabilidade de todos.

Sua atitude rápida e correta reduz
riscos, evita danos e fortalece nossa
cultura de proteção da informação.



FLUXO

1



Identificar

2



Comunicar

3



Conter

4



Investigar

5



Corrigir

6



Aprender



Agir com rapidez e responsabilidade faz toda a diferença.

Identifique, comunique e colabore.

Juntos, protegemos nossas informações e o nosso futuro.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

11.

PAPÉIS E RESPONSABILIDADES

A segurança da informação é uma responsabilidade de todos. Cada papel é essencial para proteger nossas informações e garantir a continuidade do negócio.



Segurança é compromisso coletivo.

Todos têm um papel importante para proteger nossas informações, dados e sistemas.



PAPÉIS E RESPONSABILIDADES

1



Alta Direção



2



TI



3



Jurídico & Compliance



4



Gestores



5



Colaboradores



6



Terceiros



A segurança da informação depende da atuação de todos.
Conheça seu papel, cumpra suas responsabilidades
e contribua para a proteção das nossas informações.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

12.

CANAL DE DENÚNCIAS

Nosso Canal de Denúncias é seguro, confidencial e acessível a todos. Utilize-o para reportar condutas inadequadas ou violações às nossas políticas e ao Código de Conduta.



Fale com confiança.

Sua atitude fortalece nossa integridade e contribui para um ambiente ético e seguro.



Sua voz faz a diferença.

Denuncie. Nós apuramos. Juntos, agimos.

FLUXO

- 1  Recebimento
- 2  Análise
- 3  Investigação
- 4  Tratamento
- 5  Encerramento

GARANTIAS



Confidencialidade

Sua identidade e as informações são protegidas.



Anonimato

Você pode denunciar de forma anônima.



Não Retaliação

Não toleramos qualquer forma de retaliação.



Imparcialidade

As denúncias são tratadas de forma justa, ética e independente.



Integridade se constrói com atitudes.

Denuncie condutas inadequadas. Sua atitude **protege** pessoas, informações e o nosso futuro.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE

13.

Consequências e Medidas Disciplinares

O descumprimento das nossas políticas, procedimentos e do Código de Conduta pode gerar consequências.

As medidas disciplinares são aplicadas de acordo com a **gravidade da conduta**, seu impacto e a reincidência.



Nosso compromisso com a integridade.

As medidas disciplinares reforçam nossa cultura ética e o respeito às nossas regras.



Todas as medidas são aplicadas com **imparcialidade**, respeito à legislação e garantia do contraditório e da ampla defesa.

MEDIDAS DISCIPLINARES



1. Orientação

Alinhamento e reforço das condutas esperadas.



2. Advertência Verbal

Registro da conduta inadequada e orientação sobre a correção.



3. Advertência Escrita

Registro formal da infração e comunicação por escrito.



4. Suspensão

Afastamento temporário das atividades, conforme a gravidade do caso.



5. Rescisão do contrato de trabalho ou do vínculo com a empresa

Aplicada nos casos mais graves e reincidentes.



6. Responsabilização Administrativa, Civil e Criminal

Quando a conduta configurar infração à lei ou gerar danos à empresa ou a terceiros.



Integridade não é apenas uma escolha, é o que nos fortalece.
Condutas inadequadas não serão toleradas e poderão gerar medidas disciplinares e responsabilização legal.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE



NOSSA

PERGUNTA DE OURO

Antes de agir, pergunte:



É legal?



Está de acordo com nossas políticas?



Eu me sentiria confortável se isso fosse divulgado publicamente?



Estou protegendo a reputação da Hub Health?



Se alguma resposta for

“não” ou **“não sei”**,
procure o **Jurídico & Compliance**.



ÉTICA SE PRÁTICA.



INTEGRIDADE
SE FORTALECE.



O SILÊNCIO
PERMITE.

A ATITUDE TRANSFORMA.



ÉTICA



RESPEITO



INTEGRIDADE



RESPONSABILIDADE



ELABORADO POR:

Departamento Jurídico e Compliance



REVISADO POR:

Comitê de Compliance



APROVADO POR:

Diretoria Executiva



VERSÃO: 04

DATA DE PUBLICAÇÃO:

Julho/2026