Grupo hdoc saúde

Política de **Segurança da Informação**

@grupohdocsaude

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
DATA DE EMISSÃO: 26/02/24	**DATA DE REVISÃO:**	**VERSÃO:** 1.0
ELABORADO POR: DIRETORIA DE GOVERNANÇA	**VALIDADO POR:** CONSELHO ADMINISTRATIVO	

Sumário

1. Objetivo
2. Abrangência
3. Referências
4. Atribuições e Responsabilidades
   - Conselho de Administração
   - Diretoria Executiva
   - Diretoria de Governança
   - Diretoria Jurídica
   - Gestão de TI
   - Diretor Administrativo
   - Demais Líderes e Gestores
   - Colaboradores
5. Diretrizes da Política
   - Importância da Informação
   - Classificação da Informação
   - Uso Seguro de Dados
6. Uso dos Recursos Corporativos
   - Correio Eletrônico
   - Internet
   - Mídias Sociais
   - Ambiente Interno do Trabalho
   - Ambiente Externo
   - Computadores Corporativos
   - BYOD (Bring Your Own Device)
7. Gestão de Senhas
8. Guarda de Documentos Físicos
9. Backup
10. Uso de Inteligência Artificial
11. Norma para Uso de Certificado Digital da Diretoria
12. Canais de Comunicação e Denúncias
13. Violação e Sanções
14. Disposições Gerais

OBJETIVO

Esta Política tem como objetivo estabelecer diretrizes para proteger as informações do **Grupo HDOC**, garantindo a confidencialidade, integridade e disponibilidade dos dados. Alinha-se à Lei Geral de Proteção de Dados (LGPD), à ISO 27001 e aos princípios de Governança Corporativa, promovendo uma cultura de ética, transparência e responsabilidade. Visa mitigar riscos relacionados à segurança da informação, proteção de dados, segurança cibernética e uso de inteligência artificial, em conformidade com o Código de Conduta e Ética do **Grupo HDOC.**

ABRANGÊNCIA

Aplica-se a todos os usuários com acesso às informações do **Grupo Hdoc Saúde** e empresas do grupo, independente do seu vínculo com a empresa, ou seja, gestor, colaborador, estagiário, temporário, terceiro, prestador de serviço ou de qualquer forma no âmbito de Representante e/ou Parceiro de Negócios.

REFERÊNCIAS

Constituição Federal da República Federativa do Brasil (1988): Princípios fundamentais sobre privacidade, inviolabilidade da intimidade e proteção de dados pessoais.

Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD): Estabelece regras para o tratamento de dados pessoais, incluindo princípios, direitos dos titulares e obrigações dos agentes de tratamento.

Decreto nº 8.771/2016: Regulamenta o Marco Civil da Internet, detalhando medidas de segurança e proteção de dados pessoais.

ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação (SGSI): Norma internacional que define requisitos para estabelecer, implementar, manter e melhorar continuamente a segurança da informação.

ISO/IEC 27701:2020 – Sistema de Gestão de Privacidade da Informação: Extensão da ISO 27001, com foco em práticas de proteção da privacidade e gestão de dados pessoais.

Código das Melhores Práticas de Governança Corporativa (6ª Edição, IBGC): Estabelece princípios e práticas para a governança corporativa, com foco em transparência, equidade, prestação de contas e responsabilidade corporativa.

Regulamento Europeu de Proteção de Dados (GDPR – General Data Protection Regulation): Referência internacional para práticas de proteção de dados pessoais, especialmente aplicável em casos de transferência internacional de dados.

ATRIBUIÇÕES E RESPONSABILIDADES

Conselho de Administração	Aprovar esta política e suas atualizações, garantir a alocação de recursos necessários para a segurança da informação, supervisionar a eficácia dos controles de governança e segurança por meio de comitês de auditoria e compliance.
Diretoria Executiva	Promover a cultura de segurança da informação, garantir o alinhamento da política com a estratégia do Grupo HDOC, apoiar iniciativas de gestão de riscos e assegurar a implementação de controles adequados para proteção das informações.
Diretoria de Governança	Definir diretrizes de governança da informação, acompanhar a aderência às melhores práticas de segurança e compliance, apoiar a gestão de riscos corporativos e monitorar a efetividade dos processos relacionados à segurança da informação.
Diretoria Jurídica	Orientar sobre a conformidade legal da política, garantir o alinhamento com a LGPD e demais legislações aplicáveis, assessorar em casos de incidentes de segurança e atuar como suporte jurídico em questões de proteção de dados.
Gestão de TI	Implementar e manter controles técnicos para garantir a confidencialidade, integridade e disponibilidade das informações, monitorar riscos cibernéticos e responder a incidentes de segurança da informação de forma proativa.
Diretor Administrativo	Assegurar a implementação das diretrizes de segurança da informação nas áreas administrativas, gerenciar riscos operacionais relacionados à segurança da informação e promover a conscientização dos colaboradores sobre boas práticas.
Demais Líderes e Gestores	Disseminar as diretrizes da política entre suas equipes, garantir o cumprimento das normas de segurança da informação em suas áreas de atuação e identificar, avaliar e reportar riscos relacionados à proteção de dados e informações.
Colaboradores	Cumprir as diretrizes estabelecidas nesta política, adotar práticas seguras no uso e tratamento de informações, proteger dados confidenciais e reportar imediatamente qualquer incidente ou suspeita de violação de segurança da informação.

Diretrizes da Política

Importância da Informação

A informação é um dos ativos mais valiosos do **Grupo HDOC Saúde**, fundamental para a continuidade dos negócios, a tomada de decisões estratégicas e a manutenção da confiança de clientes, parceiros e stakeholders. A proteção adequada da informação contribui para a resiliência operacional, a segurança jurídica e a preservação da reputação da organização.

Classificação da Informação

Para garantir a proteção adequada, as informações do **Grupo HDOC Saúde** devem ser classificadas com base em seu grau de sensibilidade e impacto potencial em caso de divulgação não autorizada:

- **Informação Pública:** Dados que podem ser divulgados sem restrição, como relatórios anuais e comunicados oficiais.
- **Informação de Uso Interno:** Dados destinados exclusivamente aos colaboradores do Grupo HDOC, cuja divulgação externa não é permitida sem autorização prévia.
- **Informação Confidencial:** Informações sensíveis que, se expostas, podem causar prejuízos financeiros, operacionais ou de imagem, como contratos, dados de clientes e estratégias comerciais.
- **Informação Sigilosa:** Dados críticos cuja divulgação não autorizada pode comprometer a segurança da organização, incluindo informações de segurança cibernética, planos estratégicos e informações protegidas por leis específicas.

Diretrizes para o Uso Seguro de Dados

O uso seguro das informações é uma responsabilidade de todos os colaboradores do **Grupo HDOC**. Para garantir a proteção dos dados, devem ser seguidas as seguintes diretrizes:

- As informações de propriedade do Grupo Hdoc Saúde devem ser protegidas de riscos e ameaças que possam comprometer a confidencialidade, sigilo, integridade ou disponibilidade destas.
- Seu compartilhamento, ainda que no âmbito do próprio Grupo Hdoc Saúde, deve ocorrer apenas com aqueles que necessitem conhecê-las.
- Os administradores e colaboradores não devem manipular nem se valer de dados sobre as atividades do Grupo Hdoc Saúde que possam influenciar decisões em proveito pessoal, ou gerar benefício ou prejuízo a terceiros, sob pena de responsabilidade civil e criminal.
- Informações classificadas como estratégicas deverão receber tratamento sigiloso. Estas só podem ser divulgadas com autorização do Diretor Executivo ou em caso de exigência legal ou decisão judicial.
- O colaborador, mesmo após estar desvinculado ao Grupo Hdoc Saúde, não poderá utilizar para fins particulares, nem repassar a outrem, quaisquer informações que pertençam ao Grupo.

- **Conscientização Contínua:** Participar de treinamentos e ações de conscientização sobre segurança da informação e proteção de dados, promovendo uma cultura organizacional voltada para a segurança.
- **Relato de Incidentes:** Reportar imediatamente qualquer incidente de segurança da informação, como perda de dispositivos, acessos não autorizados ou suspeitas de violação de dados.

A classificação deverá ser realizada no momento em que a informação/dado for gerada ou, posteriormente, sempre que necessário.
Na hipótese de documento que contenha informações classificadas em diferentes tipos será atribuído ao documento o tratamento de sigilosa, ficando assegurado o acesso apenas após aprovação do Executivo responsável pela informação.

As informações que não possuem uma classificação explícita são classificadas como Uso Interno, e caso seja identificada como Dado Pessoal e Dado Pessoal Sensível, nos termos da Lei Federal nº 13.709/2018, que dispõe sobre a proteção de dados pessoais, será classificada como Confidencial.

USO DO CORREIO ELETRÔNICO

O uso do correio eletrônico é voltado exclusivamente para fins corporativos e relacionados às atividades do colaborador dentro do **Grupo Hdoc Saúde.**

É vedado utilização de e-mails corporativo para cadastro em sites externos que não estejam relacionados aos processos da empresa e para fins corporativos (ex.: Blogs, fóruns, jogos, redes sociais, sites de compras etc.).

Toda comunicação de e-mails com parceiros, fornecedores ou clientes, devem ser obrigatoriamente realizados através de e-mails corporativos.

O **Grupo Hdoc Saúde** se reserva o direito de rastrear, monitorar, gravar e inspecionar quaisquer informações transmitidas via e-mail corporativo.

USO DA INTERNET

A Internet corporativa deve ser utilizada exclusivamente para fins corporativos, enriquecimento intelectual ou como ferramenta de busca por informações, enfim, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

O uso da internet para assuntos pessoais é permitido, com limitações, desde que com bom senso e respeitando os princípios e regras definidas no Código de Conduta e Ética do **Grupo Hdoc Saúde** e seus demais regulamentos.

Não é permitido os acessos a sites impróprios na Internet, incluindo, mas não se limitando a: jogos, mensagens de corrente, troca ou armazenamento de conteúdo ilícito, obsceno, pornográfico, violento, discriminatório, racista, difamatório ou que desrespeite qualquer indivíduo ou entidades, de acordo com as Leis nº 8.069 (Estatuto da Criança e do Adolescente) e nº 12.965 (Marco Civil da Internet).

Os acessos a internet corporativa são monitorados através de identificação do usuário, podendo ser bloqueados a qualquer momento, sem aviso prévio, pela equipe de tecnologia ou segurança da informação, quando for identificado alguma irregularidade ou risco ao ambiente.;

USO DE MÍDIAS SOCIAIS

Todos os assuntos relacionados a comunicação externa e mídias sociais devem ser centralizado nas áreas marketing, comunicação ou áreas formalmente autorizadas, desta forma nenhum colaborador, terceiro, prestador de serviços e/ou parceiros pode através de meios de comunicação, mídias sociais ou sites externos, publicar, comentar ou ter atitudes semelhantes, em nome do **Grupo Hdoc Saúde**, sem autorização formal.

O uso dos recursos tecnológicos e de comunicação deve ser restrito a temas pertinentes ao trabalho, podendo, a qualquer tempo, ser auditado pelo Grupo Hdoc Saúde. Não é permitido divulgar/compartilhar em redes sociais opiniões em nome do **Grupo Hdoc Saúde.**

É proibido a divulgação de informações sensíveis do Grupo. Além disso, não é permitido utilizar linguagem ofensiva às nossas marcas, recomendando-se que os mesmos critérios sejam adotados pelos parceiros comerciais e equipe de trabalho.

AMBIENTE INTERNO DO TRABALHO

É necessário observar o ambiente antes de falar/tratar assuntos relevantes e/ou informações sensíveis da Empresa, devendo ser observadas as seguintes regras:

Nunca divulgar ou compartilhar qualquer informação ou dado do **Grupo Hdoc Saúde** sem prévia autorização da alçada competente;
Evitar a divulgação de informações sensíveis, mesmo que nas dependências das instalações do Grupo, em ambientes abertos.

Apenas a área responsável pela produção da informação ou que possui atribuição para tratar da matéria, poderá divulgá-la e discuti-la internamente; Observar em documentos eletrônicos, impressos, a cautela no seu compartilhamento (destinatários de e-mail e guarda de documentos impressos); Proteger senhas e acessos aos sistemas eletrônicos do **Grupo Hdoc Saúde**, sendo terminantemente proibido o seu compartilhamento.

DO AMBIENTE EXTERNO

O cuidado com a informação do **Grupo HDOC** deve ser mantido em qualquer ambiente, especialmente fora das dependências da organização. Em locais públicos, como aeroportos, cafés, transportes públicos, hotéis ou eventos externos, é fundamental adotar medidas preventivas para evitar o acesso não autorizado ou a exposição acidental de informações sensíveis.

Os colaboradores devem evitar discutir informações confidenciais em locais públicos ou por meio de chamadas telefônicas em ambientes abertos. O uso de dispositivos eletrônicos em áreas externas deve ser realizado com atenção redobrada. Além disso, recomenda-se o uso de redes seguras, evitando conexões públicas não protegidas sem a devida utilização de VPN (Virtual Private Network).

Documentos impressos ou digitais contendo informações confidenciais devem ser transportados de forma segura e nunca deixados desacompanhados em locais públicos. Em situações de reuniões externas, é importante garantir que apenas pessoas autorizadas tenham acesso às informações compartilhadas, com a adoção de medidas de controle de acesso quando aplicável.

O descuido em ambientes externos pode resultar em perdas significativas para a organização, incluindo danos à reputação, prejuízos financeiros e violações de conformidade legal. Por isso, a responsabilidade pela proteção das informações do **Grupo HDOC** se estende além do ambiente corporativo, sendo um compromisso contínuo de todos os colaboradores.

USO DE COMPUTADORES CORPORATIVOS

Os recursos corporativos devem ser utilizados com responsabilidade e exclusivamente para atividades relacionadas a empresa. Os usuários devem ter zelo pelos recursos corporativos, como computadores, impressoras, celulares e demais equipamentos, podendo sofrer sanções administrativas.
Não é permitido que usuários sejam administradores de suas máquinas, exceções devem ser avaliadas, justificadas e documentadas;

Não é permitido instalar ou executar softwares não licenciados, ou considerados "piratas", assim como softwares não homologados nos ativos corporativos. A imagem do sistema operacional dos equipamentos corporativos deve ser padronizada e homologada pela equipe de Tecnologia da Informação, devendo ser atualizada periodicamente e mantendo sempre as atualizações de segurança mais recentes.

A manutenção e configuração dos computadores corporativos é de responsabilidade exclusiva da equipe de Tecnologia da Informação, sendo vedado aos demais colaboradores alterarem suas configurações, abrir o equipamento ou alterar componentes, sem autorização formal. Todos os incidentes corporativos que envolvam as máquinas corporativas, incluindo, mas não se limitando a vulnerabilidades, vírus de computador e ataques digitais diretos ou indiretos, devem ser reportados imediatamente para a equipe de Tecnologia da Informação.

BYOD

O uso de dispositivos pessoais para fins profissionais, conhecido como BYOD (Bring Your Own Device), é permitido no **Grupo HDOC**, desde que em conformidade com as diretrizes de segurança da informação estabelecidas nesta política. O acesso a informações corporativas por meio de dispositivos pessoais, como smartphones, tablets e laptops, deve ser autorizado previamente pela área de TI e estar condicionado à implementação de controles de segurança adequados.

É proibido o armazenamento de informações confidenciais ou sensíveis em dispositivos pessoais sem autorização prévia. Caso haja necessidade de armazenar dados corporativos, medidas adicionais de segurança, como criptografia, devem ser adotadas. Em caso de perda, roubo ou comprometimento do dispositivo, o colaborador deve notificar imediatamente a área de TI para que sejam tomadas as providências necessárias para proteger as informações.

É proibido o armazenamento de informações confidenciais ou sensíveis em dispositivos pessoais sem autorização prévia. Caso haja necessidade de armazenar dados corporativos, medidas adicionais de segurança, como criptografia, devem ser adotadas. Em caso de perda, roubo ou comprometimento do dispositivo, o colaborador deve notificar imediatamente a área de TI para que sejam tomadas as providências necessárias para proteger as informações.

PROPRIEDADE INTELECTUAL

Todos os bens materiais físicos ou lógicos, gerados ou desenvolvidos pelos colaboradores, terceiros, prestadores de serviço e parceiros, no exercício de suas atribuições, utilizando recursos tecnológicos da empresa, mesmo que fora do horário de trabalho, são de propriedade exclusiva do **Grupo Hdoc Saúde**.
Ex.: Informações, documentos (físicos ou lógicos), assistentes de inteligência artificial, criações, inventos, desenvolvimentos, aperfeiçoamentos ou outras melhorias feitas, armazenados, produzidos ou transformados.

Todo usuário é responsável pela preservação da propriedade intelectual da organização, bem como pela observância e respeito à propriedade intelectual de terceiros, nos termos da legislação vigente, cabendo à responsabilização em casos de omissão, dolo ou culpa. Todas as informações que pertençam à empresa, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

DA GESTÃO DE SENHAS

A gestão de senhas é essencial para garantir a proteção dos sistemas e informações do **Grupo Hdoc Saúde**. Todos os colaboradores devem seguir as diretrizes de segurança para criação, armazenamento e uso de senhas, garantindo que acessos não sejam comprometidos.
As senhas devem ser únicas, complexas e atualizadas regularmente. Recomenda-se o uso de pelo menos 8 caracteres, combinando letras maiúsculas e minúsculas, números e símbolos especiais. O uso de senhas óbvias ou fáceis de adivinhar, como datas de nascimento ou sequências numéricas simples, é estritamente proibido.
As senhas devem ser armazenadas de maneira segura e nunca compartilhadas com terceiros. O uso de gerenciadores de senhas é recomendado para manter a segurança e evitar reutilização indevida.
O descumprimento das diretrizes de gestão de senhas pode resultar em vulnerabilidades e comprometimento da segurança das informações. Qualquer suspeita de comprometimento de credenciais deve ser reportada imediatamente à equipe de TI para a adoção de medidas corretivas adequadas.
Todas as informações do **Grupo Hdoc Saúde** devem receber uma classificação, assim como um nível adequado de proteção, de acordo com o seu valor, grau de sigilo, sensibilidade e criticidade para o negócio.
Todas as informações do **Grupo Hdoc Saúde** devem ser manuseadas e armazenadas somente em computadores corporativos e/ou nuvem privada oficiais da empresa. Não é permito manusear, armazenar e transferir informações, sem autorização, para dispositivos ou meios de armazenamento externos, assim como ambientes de armazenamento em nuvens que não sejam da empresa (Dropbox, OneDrive, iCloud, Google Drive, dentre outros).
Os ativos associados com informações corporativas devem ser identificados e inventariados. Para todo ativo, deve ser definido um responsável, independente do seu meio de acesso, seja em sistemas, servidor ou banco de dados, mantendo a proteção adequada de acordo com a grau de risco, assim como as aprovações corretas de acessos;

É estritamente proibido a utilização de dispositivos vinculados à Tecnologia de Informação (servidores, banco de dados, roteadores, softwares de desenvolvimento etc.) que não sejam gerenciados e homologados pela área de TI ou segurança da informação;

Os recursos tecnológicos corporativos devem ter minimamente implementado:

• Todos os servidores devem ser monitorados constantemente para a eliminação de vulnerabilidades de segurança, bem como a aplicação de correções de segurança reportadas;

• Segregação de rede, seja esta física ou lógica, através dos mecanismos e tecnologias aplicáveis, assegurando a confidencialidade, integridade e disponibilidade das informações trafegadas;

• Softwares de antivírus em todas as estações de trabalho e servidores, com processos estabelecidos que garantam as atualização e execuções adequadas;
• Proteção de e-mails (anti-spoofing, filtro de reputação, AntiSpam, anti-phishing);

• Equipamentos que estabeleçam barreiras de segurança (Firewalls e WAF);

• Mecanismos de detecção de intrusos devem ser adotados em todas as comunicações da rede corporativa com o meio externo;

• Os computadores de usuários devem dispor de recursos de firewall pessoal, bem como configurações de segurança, a atualização de patches, visando à redução de chances de invasões, evasão de informações e/ou acessos não autorizados;

• Controles tecnológicos devem ser implementados visando monitorar, proteger e minimizar os riscos associados às informações ou ativos de processamento, de modo a preservar suas propriedades de confidencialidade, integridade e disponibilidade.

• Estes controles devem atuar na prevenção, restrição, monitoração e detecção de incidentes de segurança. Os relógios dos ambientes e sistemas corporativos, devem ser sincronizados com uma fonte de tempo precisa e única para todos;

• Todas as ocorrências de fraudes ou suspeitas devem ser investigadas, registradas e tratadas de forma condizente à dimensão da situação. Deve ser instituído um canal para denúncias no sentido de obter contribuições voluntárias para a identificação e a eliminação de potenciais fraudes ou desvios de comportamento identificadas pelos colaboradores, prestadores de serviço ou clientes.

DA GUARDA DE DOCUMENTOS FÍSICOS

A guarda de documentos físicos do **Grupo HDOC** deve ser realizada de forma a garantir a integridade, confidencialidade e disponibilidade das informações, em conformidade com as normas de segurança da informação e regulamentos aplicáveis. Os documentos devem ser armazenados em locais seguros, com acesso restrito a pessoas autorizadas, utilizando armários, cofres ou arquivos trancados quando necessário.

É fundamental que documentos classificados como confidenciais ou sigilosos estejam protegidos contra riscos de perda, furto, danos acidentais, incêndios ou desastres naturais. Para isso, devem ser adotadas medidas de segurança física, como controle de acesso às áreas de arquivamento, uso de sistemas de monitoramento e protocolos de segurança específicos.

O acesso a documentos físicos deve ser registrado e monitorado, especialmente para informações sensíveis. Documentos em trânsito entre unidades, departamentos ou terceiros devem ser transportados de forma segura, com o devido acompanhamento e proteção contra acessos não autorizados.

O descarte de documentos físicos que contenham informações sensíveis deve ser realizado de forma segura, preferencialmente por meio de trituração ou outros métodos que impossibilitem a reconstrução das informações. O processo de descarte deve ser documentado e supervisionado para garantir a conformidade com as políticas internas.

O descumprimento das diretrizes para a guarda de documentos físicos pode resultar em sanções disciplinares, bem como em responsabilizações civis, administrativas ou criminais, dependendo da gravidade da violação.

DO BACKUP

Todas as ocorrências de fraudes ou suspeitas devem ser investigadas, registradas e tratadas de forma condizente à dimensão da situação. Deve ser instituído um canal para denúncias no sentido de obter contribuições voluntárias para a identificação e a eliminação de potenciais fraudes ou desvios de comportamento identificadas pelos colaboradores, prestadores de serviço ou clientes.

A gestão de backup é fundamental para garantir a disponibilidade e a recuperação das informações do **Grupo HDOC** em casos de falha, incidente de segurança ou desastre. Todos os backups devem ser realizados conforme as diretrizes de segurança da informação, garantindo a integridade e a proteção dos dados armazenados.

Os backups devem ser periódicos, seguindo um cronograma previamente definido e aprovado pela área de TI. As cópias de segurança devem ser armazenadas em locais seguros, preferencialmente utilizando criptografia para evitar acessos não autorizados. Sempre que possível, deve-se manter redundância, com armazenamento em diferentes locais, incluindo ambientes na nuvem e servidores físicos protegidos.

A restauração de backups deve ser testada regularmente para garantir a efetividade do processo e a recuperação dos dados sem perdas. Apenas profissionais autorizados devem ter acesso às cópias de segurança, sendo vedado o uso de dispositivos pessoais para armazenamento de backups corporativos.

O descumprimento das diretrizes de gestão de backup pode comprometer a continuidade dos negócios e resultar em perda irreversível de informações. Qualquer incidente relacionado a falhas de backup deve ser reportado imediatamente à equipe de TI para investigação e correção.

DO USO DA INTELIGÊNCIA ARTIFICIAL

O uso de Inteligência Artificial (IA) no Grupo HDOC deve seguir princípios éticos, legais e de segurança da informação, garantindo transparência, privacidade e conformidade com as regulamentações vigentes. O desenvolvimento, implementação e utilização de soluções baseadas em IA devem ser supervisionados por equipes qualificadas e alinhados às diretrizes corporativas de segurança e governança de dados.

Todas as soluções de IA utilizadas devem respeitar os direitos dos titulares de dados, garantindo que não haja viés discriminatório, uso indevido de informações sensíveis ou impactos negativos à privacidade. Os modelos de IA devem ser monitorados continuamente para evitar falhas e assegurar a precisão dos resultados. Além disso, é obrigatória a revisão humana nos processos em que a IA impacte decisões estratégicas, operacionais ou que possam gerar efeitos significativos sobre clientes, colaboradores ou parceiros.

O acesso a dados para treinamento e uso de IA deve ser controlado, garantindo que apenas informações necessárias sejam utilizadas, sempre com medidas de proteção adequadas, como anonimização e criptografia. Além disso, qualquer solução de IA que impacte diretamente processos críticos da empresa deve passar por avaliação prévia de riscos e ser aprovada pelos comitês responsáveis.

O **Grupo HDOC** poderá monitorar o uso de inteligência artificial por meio dos recursos tecnológicos disponibilizados pela empresa, assegurando que seu uso esteja em conformidade com as políticas internas e regulamentos aplicáveis. Esse monitoramento tem como objetivo prevenir riscos operacionais, proteger informações sensíveis e garantir que a IA seja utilizada de forma segura e ética.

O descumprimento desta norma pode resultar em impactos negativos à segurança e à reputação da organização, além de possíveis sanções legais e administrativas. Qualquer incidente relacionado ao uso de IA deve ser imediatamente reportado para análise e mitigação de riscos.

O uso de Inteligência Artificial (IA) no **Grupo HDOC** deve seguir princípios éticos, legais e de segurança da informação, garantindo transparência, privacidade e conformidade com as regulamentações vigentes. O desenvolvimento, implementação e utilização de soluções baseadas em IA devem ser supervisionados por equipes qualificadas e alinhados às diretrizes corporativas de segurança e governança de dados.
Todas as soluções de IA utilizadas devem respeitar os direitos dos titulares de dados, garantindo que não haja viés discriminatório, uso indevido de informações sensíveis ou impactos negativos à privacidade. Os modelos de IA devem ser monitorados continuamente para evitar falhas e assegurar a precisão dos resultados.

O acesso a dados para treinamento e uso de IA deve ser controlado, garantindo que apenas informações necessárias sejam utilizadas, sempre com medidas de proteção adequadas, como anonimização e criptografia. Além disso, qualquer solução de IA que impacte diretamente processos críticos da empresa deve passar por avaliação prévia de riscos e ser aprovada pelos comitês responsáveis.

O **Grupo HDOC** poderá monitorar o uso de inteligência artificial por meio dos recursos tecnológicos disponibilizados pela empresa, assegurando que seu uso esteja em conformidade com as políticas internas e regulamentos aplicáveis. Esse monitoramento tem como objetivo prevenir riscos operacionais, proteger informações sensíveis e garantir que a IA seja utilizada de forma segura e ética.

O descumprimento desta norma pode resultar em impactos negativos à segurança e à reputação da organização, além de possíveis sanções legais e administrativas. Qualquer incidente relacionado ao uso de IA deve ser imediatamente reportado para análise e mitigação de riscos.

DA NORMA PARA USO DE CERTIFICADO DIGITAL DA DIRETORIA

O uso de certificados digitais pela Diretoria do **Grupo HDOC** é obrigatório para garantir autenticidade, integridade e validade jurídica em documentos e transações eletrônicas. Os certificados digitais devem ser emitidos por Autoridades Certificadoras reconhecidas e utilizados exclusivamente para fins institucionais, conforme as diretrizes estabelecidas pela organização.

O certificado digital da Diretoria poderá ser utilizado por colaboradores designados para assinar documentos e realizar transações em nome da empresa, desde que previamente autorizados e com os devidos controles de segurança implementados.

Cada membro da Diretoria e colaborador autorizado é responsável pelo uso seguro do certificado digital, devendo protegê-lo com senhas robustas e armazená-lo em dispositivos seguros, como tokens criptográficos ou cartões inteligentes. O compartilhamento de credenciais ou o uso indevido do certificado digital é estritamente proibido e pode resultar em sanções disciplinares.

A expiração, revogação ou substituição de um certificado digital deve ser comunicada imediatamente à área de Tecnologia da Informação para atualização dos registros e prevenção de impactos operacionais. Qualquer incidente relacionado ao uso do certificado digital deve ser reportado à equipe responsável para investigação e adoção de medidas corretivas.

O uso inadequado do certificado digital pode comprometer a segurança jurídica e a confiabilidade das transações eletrônicas, tornando essencial a conformidade com esta norma para garantir a proteção das informações e a credibilidade da organização.

O uso de certificados digitais pela Diretoria do **Grupo HDOC** é obrigatório para garantir autenticidade, integridade e validade jurídica em documentos e transações eletrônicas. Os certificados digitais devem ser emitidos por Autoridades Certificadoras reconhecidas e utilizados exclusivamente para fins institucionais, conforme as diretrizes estabelecidas pela organização.

Cada membro da Diretoria é responsável pelo uso seguro de seu certificado digital, devendo protegê-lo com senhas robustas e armazená-lo em dispositivos seguros. O compartilhamento de credenciais ou o uso indevido do certificado digital é estritamente proibido e pode resultar em sanções disciplinares.

A expiração, revogação ou substituição de um certificado digital deve ser comunicada imediatamente à área de Tecnologia da Informação para atualização dos registros e prevenção de impactos operacionais. Qualquer incidente relacionado ao uso do certificado digital deve ser reportado à Diretoria de Governança para investigação e adoção de medidas corretivas.

O uso inadequado do certificado digital pode comprometer a segurança jurídica e a confiabilidade das transações eletrônicas, tornando essencial a conformidade com esta norma para garantir a proteção das informações e a credibilidade da organização.

CANAIS DE COMUNICAÇÃO E DENÚNCIAS

Devem ser estabelecidos canais de comunicação específicos, possibilitando aos colaboradores (funcionários e prestadores de serviço), os meios necessários à realização de denúncias sobre a não aderência aos princípios desta política ou outras situações que ponham em risco a segurança organizacional da empresa.

VIOLAÇÃO E SANÇÕES

Os princípios estabelecidos nesta política possuem total aderência da Alta Administração da Organização e devem ser observados por todos do **Grupo Hdoc Saúde,** na execução de suas funções. Em nenhuma hipótese será admitida a alegação de desconhecimento para o não cumprimento desta política e derivadas.

Deve ser estabelecido procedimentos disciplinares formais para colaboradores, terceiros e prestadores de serviços, que venham a cometer infrações, violações ou incidentes graves de segurança, derivados ao não cumprimento das diretrizes descritas nesta política e derivadas, assim como o Código de Conduta e Ética.

São consideradas também violações a esta política as seguintes situações:

- Uso indevido e divulgação não autorizada de informações, segredos comerciais ou outras informações sem autorização formal;
- Uso ilícito de dados, informações, equipamentos, sistemas e demais recursos tecnológicos, incluindo a violação de leis, regulamentos internos e externos;
- Qualquer situação que exponha o **Grupo Hdoc Saúde** a perdas financeiras ou de imagem, em decorrência da quebra da confidencialidade, integridade ou disponibilidade das suas informações ou das quais que detenham custódia.

Todos os colaboradores, terceiros e prestadores de serviço devem estar cientes de que o não cumprimento das diretrizes desta política implicará em sanções, sejam internas, administrativas, legais e/ou penais, dependendo do grau da infração.

Para terceiros e prestadores de serviços, inclui-se a rescisão de contratos e penas de responsabilidade civil e criminal na máxima extensão que a lei permitir. Ao detectar uma violação, o usuário deve comunicar aos responsáveis pela Segurança da Informação imediatamente. Caso seja verificado que o colaborador não comunicou a infração, este sabendo da sua existência, o mesmo pode ser considerado coautor da mesma e assim ser indiciado e sofrer sanções.

As medidas de consequências adotadas pelo Grupo Hdoc Saúde, seja no âmbito disciplinar e interno, e/ou por meio de adoção de medida judicial cabível, serão aplicadas, após a avaliação da gravidade do caso concreto e dos impactos causados pela violação.

DISPOSIÇÕES GERAIS

Aplicabilidade. Esta Política se aplica, irrestritamente, a todos os administradores, colaboradores, acionistas, prestadores de serviços e parceiros do **Grupo Hdoc Saúde.**

Comprometimento com Confidencialidade e Sigilo. Todos os administradores e colaboradores devem ler e compreender as diretrizes e as regras instituídas nesta política. Os diretores executivos, gestores e colaboradores devem dar aceite no "Termo de Compromisso de Confidencialidade e Sigilo" renovado anualmente.

Vigência e aprovação. Esta Política tem vigência a partir da data de sua aprovação pela Diretoria Executiva por 2 (dois) anos, podendo ser revisada sempre que necessário.

Grupo hdoc saúde

@grupohdocsaude