dr.online	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
Identificação:	**Versão:**	**Nº de Páginas**	**Data:**
POL-TI-01	01	Página **1** de **12**	11/03/2026

HISTÓRICO:			
EMISSÃO INICIAL ELABORADO POR:	**ANALISADO POR:**	**APROVADO POR:**	**DATA:**
Igor Alves Pedrosa	Faranio Souza	Faranio Souza	24/03/2025

DATA:	VERSÃO:	REVISADO POR:	APROVADO POR:	ITEM REVISADO:
24/03/2025	00	Hugo Gomes	Faranio Souza	Emissão Inicial
11/03/2026	01	Data Guide	Dennis Pedroso	Incluídas diretrizes gerais e específicas.

1. OBJETIVO

O objetivo desta Política de Segurança da Informação (“PSI”) consiste em estabelecer regras de boas práticas de tratamento de dados, determinar as medidas de segurança, técnicas e administrativas para proteger os Dados Pessoais, e, ainda, garantir a confidencialidade, integridade, disponibilidade e proteção das informações da Dr. Online. Além disso, visa proteger os dados e informações da Dr. Online contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2. ESCOPO E APLICAÇÃO

Esta Política aplica-se a todos os colaboradores, prestadores de serviço, profissionais autônomos, ou pessoas autorizadas a ter acesso às informações, dados pessoais e/ou recursos de tecnologia da Dr. Online e/ou de seus clientes, de acordo com as permissões a ele atribuídas, com ênfase nas seguintes frentes:

- Tecnologia da Informação: infraestrutura de rede, sistemas, suporte e segurança da informação;
- Processos organizacionais que envolvam coleta, tratamento, armazenamento e compartilhamento de dados.

3. BASE LEGAL E NORMATIVA

- Lei no 13.709/2018 – Lei Geral de Proteção de Dados (LGPD);
- Decreto-Lei no 5.452/1943 – Consolidação das Leis do Trabalho (CLT);
- ISO/IEC 27001 – Sistemas de Gestão de Segurança da Informação.

4. DEFINIÇÕES E TERMOS

Ativo: qualquer coisa que tenha valor para a organização, a exemplo de: instalações, informação, software, hardware, mas também em pessoas, habilidades, experiência e coisas intangíveis, como reputação e também imagem.

Colaborador: Empregado, estagiário, temporário e/ou menor aprendiz ou qualquer outro indivíduo que tenha relação de trabalho com a Dr. Online

Confidencialidade: propriedade em que a informação ou dado pessoal não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados.

Dados Pessoais: informação relacionada a pessoa natural identificada ou identificável.

Disponibilidade: característica de ser acessível e utilizável sob demanda por uma entidade autorizada.

Encarregado pelo Tratamento de Dados Pessoais ou "Encarregado": pessoa física ou jurídica indicada pelo controlador e operador, para atuar como canal de comunicação com os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

Incidente de Segurança da Informação: é qualquer evento adverso identificado que indique possível violação dos dados e informações no que diz respeito a propriedades de confidencialidade, integridade ou disponibilidade da informação, falha de controles ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Informação: conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato. Não necessariamente precisa envolver dados pessoais. Exemplo: incidente envolvendo dados financeiros da Dr. Online.

Prestador de Serviço: pessoa jurídica que é contratada para realizar uma atividade específica ou fornecer um serviço determinado, que se compromete com o cumprimento desta Política.

Usuários: são todos os Colaboradores, Prestadores de Serviços, profissionais autônomos, ou pessoas autorizadas a ter acesso às informações, Dados Pessoais e/ou recursos de tecnologia da Dr. Online, de acordo com as permissões a ele atribuídas.

5. DIRETRIZES GERAIS

- Toda informação produzida ou recebida pelos usuários como resultado da atividade profissional pertence ao Dr. Online.
- Os equipamentos de informática e comunicação, sistemas e informações devem ser utilizados somente para a realização das atividades profissionais.
- Todo o uso dos sistemas e serviços deve ser registrado visando garantir a disponibilidade e a segurança das informações utilizadas.

- A fim de reduzir possíveis riscos, todos os usuários devem ser orientados sobre as políticas de segurança da informação e uso correto dos recursos, já na fase de onboarding.
- Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação do ambiente de produção.
- Devem ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a empresa julgar necessário para reduzir os riscos dos seus ativos de informação.
- A empresa exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus usuários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.
- O não cumprimento dos requisitos previstos acarreta violação às regras internas da empresa e sujeita o usuário às medidas administrativas e legais cabíveis.

6. DIRETRIZES ESPECÍFICAS

6.1 Identificação e autenticação de usuário

- A cada usuário autorizado deve ser atribuído um identificador único (login e senha) para uso pessoal e exclusivo, como um mecanismo para controlar, monitorar e proteger seu acesso a sistemas e informações, e não devem ser compartilhados com outras pessoas (usuários) em nenhuma hipótese.
- Não deve existir de forma nenhuma, login pessoal de uso compartilhado. Sendo que, a responsabilidade perante a empresa e a legislação (cível e criminal) será dos usuários que dele se utilizar.
- Todos os acessos (logins e senhas) devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for desligado ou pedir demissão, o setor de Recursos Humanos deve imediatamente comunicar através de e-mail tal fato ao setor de Tecnologia da Informação, a fim de que essa providência seja tomada.

  Nota: A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

6.2 Gestão de Senhas

- As senhas são confidenciais, intransferíveis e é de responsabilidade do usuário mantê-las como tal.

- O uso de senhas de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.
- O usuário pode alterar a própria senha sempre que achar necessário, e deve fazê-lo, sempre que suspeitar que terceiros obtiveram acesso indevido ao seu login/senha.
- Para configuração das senhas de acesso à Plataforma da Dr. Online, o usuário deve adotar a seguinte parametrização:

ITEM	ATRIBUTO
Tamanho da Senha:	8 caracteres - usuário comum 12 caracteres - admin
Complexidade (composição) da Senha:	Alfanumérico obrigatório, caracteres especiais e variação entre caixa-alta e caixa-baixa (maiusculo e minúsculo).
Expiração da senha (periodicidade máxima para troca das senhas):	120 dias
Histórico de senhas usadas:	4 últimas
Mudança de senha obrigatória no primeiro logon	Sim

6.3 Direitos de Acesso (permissões/privilégios)

A concessão e o uso de privilégios são restritos e controlados e devem ser concedidos conforme a necessidade de uso, devendo sempre ser observada a segregação de funções e responsabilidades.

Todo usuário que deixar a empresa (seja por demissão/pedido de desligamento ou rescisão contratual) a Área de Recursos Humanos deverá solicitar imediatamente por e-mail, especificando claramente a data e horário para execução da revogação dos acessos do respectivo usuário.

- O TI de imediato, no horário e data especificada, deve realizar a revogação dos acessos.
- Anualmente, a TI deve realizar uma revisão dos direitos de acessos dos usuários.

6.4 Gestão de ativos e Recursos tecnológicos

- Os recursos tecnológicos e ativos (como notebooks, celulares) disponibilizados aos usuários são de propriedade da empresa e destinados exclusivamente às atividades relacionadas ao trabalho, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição.

- O Dr. Online , na qualidade de proprietário dos ativos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo.
- É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do setor de TI, ou de quem este determinar.
- Arquivos pessoais e/ou não pertinentes ao negócio da empresa (fotos, músicas, vídeos, etc..) não devem ser mantidos nos drives de rede. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente sem comunicação prévia ao usuário.
- Documentos imprescindíveis para as atividades da empresa devem ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não tem garantia de backup e podem ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

É proibido o uso de computadores e recursos tecnológicos para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem a explícita autorização do proprietário.
- Tratar dados pessoais sem respaldo das bases legais estabelecidas pela Lei Geral de Proteção de Dados, cujas informações estão disponibilizadas na planilha de Mapeamento de Dados Pessoais.
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectus.
- Hospedar ou acessar sites de pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.
- Manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pelo Dr. Online .

6.5 Mesa limpa e tela protegida

- Todos os computadores quando estiverem ligados e não estiverem sendo utilizados, devem ser bloqueados (Windows: Tecla Windows + L; Mac: Control + Command + Q).
- Nunca deixe senhas, códigos ou informações sigilosas anotadas em papéis, quadros brancos ou post-its colados ao monitor.
- Todos os usuários devem configurar seus computadores com o bloqueio automático para ativar após 5 minutos de inatividade.
- Feche aplicativos e documentos sigilosos antes de compartilhar sua tela em reuniões virtuais.
- O usuário é responsável por manter os recursos de segurança do sistema operacional sempre atualizados em seu computador.

6.6 Mídias Removíveis e da porta USB

- Não é permitido utilizar equipamentos portáteis e/ou acessórios particulares conectados à rede da empresa e aos computadores, tendo em vista que a porta USB é o principal ponto de vulnerabilidade de segurança.

6.7 Uso de Softwares de Mensageria

- Deve-se priorizar o uso do sistema de mensageria disponibilizado pela organização para comunicação interna (Teams).
- O uso de sistemas de mensageria em redes de relacionamento pessoais é proibido no ambiente corporativo, por não estar relacionada às atividades laborais.
- As informações corporativas, que transitam por meio de mensagens eletrônicas, devem ser salvaguardadas e utilizadas de acordo com a finalidade estabelecida, devendo ser observadas as diretrizes estabelecidas por esta Política.

6.8 Uso de E-mail

- O uso do e-mail é disponibilizado para usuários autorizados com propósitos orientados aos negócios da empresa, e é um privilégio que pode ser cancelado a qualquer momento.
- Os usuários devem evitar clicar em links de e-mail de remetentes desconhecidos ou de empresas que não mantêm relação comercial. Em caso de dúvida, deve acionar a equipe da TI para verificação quanto à segurança de acesso ao link.
- O uso de e-mail da Dr. Online implica automaticamente na aceitação do usuário quanto ao acompanhamento, auditoria e revisão do mesmo.

- O uso do correio eletrônico (e-mail) é para fins corporativos e relacionados às atividades do usuário dentro da empresa.

- Os e-mail que estiverem ameaçando, incomodando, embaraçando, resultando em abusos, ou apresentar conteúdo implícito ou explícito de caráter pornográfico ou vulgar, são estritamente proibidos, sendo passível de punição;

- As informações corporativas, que transitam por meio de e-mail, devem ser salvaguardadas e utilizadas de acordo com a finalidade estabelecida, devendo ser observadas as diretrizes estabelecidas por esta Política.

- Critérios, cuidados e análise adequada devem ser considerados, quando enviar informações importantes, confidenciais ou de propriedade da empresa através de e-ml.
- Ao final do e-mail, após a assinatura, o usuário deverá incluir o seguinte aviso de confidencialidade:

> "*Esta mensagem, juntamente com qualquer outra informação anexada, é confidencial e protegida por lei, e somente os seus destinatários são autorizados a usá-la. Caso a tenha recebido por engano, por favor, informe o remetente e em seguida apague a mensagem, observando que não há autorização para armazenar, encaminhar, imprimir, usar, copiar o seu conteúdo*."

- A cada usuário com acesso ao e-mail corporativo, é atribuído um endereço eletrônico (e-ml) composto por: Nome + sobrenome*@dr online24h.com.br*

Exemplo: Usuário João Souza Silva terá o e-mail: *joao.silva@dr online24h.com.br*

- Os usuários do e-mail "Dr. Online" devem respeitar as seguintes orientações*:*
  - ➢ Utilizar o e-mail como recurso de comunicação e não de arquivo de documentos ou controle de processos.
  - ➢ Não usar o e-mail de outra pessoa. O uso do nome ou identificação de outra pessoa é estritamente proibido. Mantenha sempre confidencial a sua senha e identificação;
  - ➢ Deve-se evitar o envio de arquivos muito pesados por e-mail. O ideal é compartilhar o arquivo na rede para que o destinatário possa acessar o arquivo remotamente sem a necessidade de download.
  - ➢ E-mails onde não se reconhece o remetente deve ser observado com cautela e evitar clicar em link ou fazer download de arquivo anexo, uma vez que podem encaminhar para sites maliciosos ou instalar aplicativos maliciosos.
  - ➢ Não é permitido pelos canais de contato o envio de jogos, correntes de amizade, softwares não registrados ou ilegais, ou qualquer outro material que não seja

pertinente aos negócios da empresa, que possa difundir informações falsas ou congestionar a rede.

6.9 Acesso à Internet

- Durante o uso da Internet, os usuários estão proibidos de divulgar informações confidenciais, ou quaisquer outras informações de propriedade da empresa ou dos clientes que o usuário tiver acesso, como parte de seu trabalho.
- Não é permitido acessar nenhum Website que implique ou que tenha conteúdo pornográfico ou vulgar e não é permitido enviar nenhuma mensagem que implique ou tenha conteúdo de ameaça, abusivo, embaraçoso, pornográfico ou vulgar.
- É proibido fazer o download (bxa) de qualquer programa, mesmo os ligados diretamente às suas atividades, bem como, não são permitidos em hipótese alguma, efetuar upload (subida) de qualquer software licenciado a empresa ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

6.10 Classificação da Informação

É de responsabilidade do Gestor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir, levando em consideração às diretrizes legais estabelecidas no Procedimento de Classificação, Rotulagem e Manuseio.

- **Pública:** É uma informação do Grupo Hebron ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.
- **Interna:** É uma informação da Dr. Online que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços do Grupo Hebron.
- **Confidencial:** É uma informação crítica para os negócios da Dr. Online ou de seus clientes. A divulgação não autorizada desta informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais ao Dr. Online ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por colaboradores, clientes e/ou fornecedores.

- **Restrita:** É toda informação que pode ser acessada somente por usuários da Dr. Online, explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada desta informação pode causar sérios danos ao negócio e/ou comprometer a estratégia da organização.

7. RESPONSABILIDADES E DEPARTAMENTOS ENVOLVIDOS

7.1 Responsabilidades dos Usuários

- Respeitar esta Política e responder pelo descumprimento dos procedimentos aqui previstos;
- Responder pela guarda e proteção dos recursos computacionais e informações colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;
- Relatar qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, através do canal no Jira, preenchendo o formulário;
- Assegurar que as informações e dados de posse da Dr. Online ou a ela relativos sejam compartilhados somente quando autorizados pela política de classificação da informação;
- Comprometer-se em não auxiliar ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro;
- Responder pelo prejuízo ou dano que vier a provocar a Dr. Online ou a outrem, em decorrência da não obediência às diretrizes e normas aqui referidas.

7.2 Responsabilidades dos Gestores

- Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- Atribuir, na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, neste último caso quando aplicável a responsabilidade do cumprimento desta PSI;
- Conceder o acesso e definir o perfil do usuário, se necessário junto à TI;
- Revisar, a cada 6 (seis) meses, os usuários cadastrados para deliberar sobre a manutenção, revisão ou revogação dos perfis de acesso existentes;
- Solicitar o acesso a um novo usuário, nos casos aplicáveis, à TI ou área responsável e informar da sda de um usuário, a fim de se proceder à revogação;
- Autorizar as mudanças no perfil do usuário;
- Educar os usuários sobre os princípios e procedimentos de segurança da informação;
- Notificar imediatamente à TI quaisquer vulnerabilidades e ameaças à quebra de segurança;

- Advertir formalmente o Usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato à TI;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

7.3 Responsabilidades da área de Tecnologia da Informação (TI)

- Configurar equipamentos e sistemas para cumprir com os requerimentos desta PSI;
- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Garantir a segurança do acesso de Partes Externas a um sistema interno ou utilizado pela Dr. Online e manter evidências que permitam a rastreabilidade para auditoria ou investigação;
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes em sistemas desenvolvidos pela Dr. Online ou ativos (endpoints, softwares, servidores, etc) dentro do ambiente e/ou infraestrutura cibernética interna;
- Administrar, proteger e testar as cópias de segurança dos programas e dados do negócio da Dr. Online, conforme Procedimento de Backup & Restore;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio da Dr. Online;
- Proteger todos os ativos de informação da Dr. Online contra códigos maliciosos e ou vírus;
- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção;
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da Dr. Online;
- Realizar inspeções periódicas de configurações técnicas e análise de riscos;
- Garantir, assim que solicitado, a concessão do acesso ao novo usuário ou o bloqueio de acesso de usuários por motivo de desligamento da Dr. Online;
- Revisar, a cada 6 (seis) meses, os usuários cadastrados para deliberar sobre a manutenção, revisão ou revogação dos perfis de acesso existentes;
- Descartar apropriadamente as mídias contendo informações referentes a Dr. Online e sanitizar as informações lá contidas, ou, apenas sanitizar as informações referentes a Dr. Online e dados pessoais contidos em mídias que serão reutilizadas;
- Promover a conscientização dos Usuários em relação à relevância da segurança da informação;
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;
- Buscar alinhamento com as diretrizes corporativas da Dr. Online;
- Realizar, a qualquer tempo, inspeção física nas máquinas de propriedade da Dr. Online.

8. DESCARTE DE MÍDIAS E DADOS

Equipamentos e mídias corporativas deverão ser encaminhadas à TI para a sanitização da informação antes do descarte, destruição ou reutilização da mídia. Dados Pessoais deverão ser descartados conforme Política de Retenção e Descarte.

9. TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A identificação e comunicação da ocorrência ou da possibilidade de ocorrência do incidente poderá ser realizada pelos usuários internos por meio do canal do Jira (com o preenchimento de um formulário) e os terceirizados, por meio do seguinte e-mail: dpo@dronline24h.com.br.

O Gestor de TI deverá acompanhar o tratamento de incidentes relacionados à Segurança da Informação, em conjunto com o Encarregado de Dados, de acordo com a metodologia de Tratamento de Incidentes, estabelecida na **Política de Gestão de Incidentes.**

10. SANÇÕES POR DESCUMPRIMENTO

O mau uso dos recursos de tecnologia caracteriza um incidente de segurança da informação e pode resultar na aplicação de sanções legais e/ou administrativas, conforme a gravidade e impacto do incidente para a Dr. Online ou seus clientes.
As violações às disposições estabelecidas na presente Política, devidamente apuradas, poderão implicar:

a. Na aplicação das sanções previstas na legislação trabalhista, podendo ser uma advertência verbal, Advertência escrita, Suspensão ou até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo Colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado ao Dr Online, seus clientes e/ou fornecedores, entre outros.
b. Na aplicação das sanções previstas na LGPD.
c. Na aplicação das sanções previstas em contrato aos Prestadores de Serviços e estagiários.
d. Na aplicação dos procedimentos legais cabíveis.

11. DISPOSIÇÕES FINAIS

Antes de efetuar ações que possam apresentar risco potencial para as informações e sistemas do Dr. Online, o Usuário deve consultar a presente PSI, a fim de certificar-se de que a atividade é lícita e segura. Os casos não previstos, dúvidas sobre segurança da informação deverão ser encaminhados para o seguinte e-mail: dpo@dronline24h.com.br.

Esta Política entra em vigor na data de sua publicação e deve ser revisada, no mínimo, anualmente, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da Dr. Online.