

1. OBJETIVO

Direcionar com informação e conhecimento, através das políticas de segurança, os usuários de ativos e serviços da informação da D4Sign, para garantia de preservação da confidencialidade, integridade e disponibilidade.

2. APLICAÇÃO

Este procedimento é aplicado a todos que utilizam ativos e serviços de informação da D4Sign.

3. DESCRIÇÃO

3.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO - PSI

3.1.1 POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

A D4Sign tem como missão reduzir a burocracia no processo de assinaturas e documentos por meio da tecnologia, com a garantia de segurança e validade jurídica. Esse documento tem por propósito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores e partes interessadas da D4Sign adotar padrões de comportamento seguro, adequados às suas metas e necessidades;

Este documento se aplica a todos os usuários da informação da D4Sign, incluindo qualquer indivíduo ou organização que possui ou já possuíram vínculo com a D4Sign, tais como prestadores de serviço, colaboradores, que possuíram, possuem ou virão a possuir acesso às informações e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura D4Sign.

O objetivo da gestão de Segurança da Informação é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na instituição.

As violações, mesmo que por mera omissão ou tentativa não consumada deste documento, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa. Os usuários

Elaboração: Fábio Oliveira	Aprovação: Rafael Figueiredo	Revisão: 01 Data: 18/07/2025
----------------------------	------------------------------	---------------------------------

estão cientes de que serão responsabilizados legalmente pelos atos, arcando com custos que possíveis incidentes possam ocasionar.

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma é obrigação do usuário da informação da D4Sign adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações.

As diretrizes detalhadas de cada requisito estão descritas nas políticas de acordo com seu tema principal, descrevendo abaixo regras gerais da segurança da informação.

3.1.2 POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Para efeitos de classificação da informação, a D4Sign utiliza as seguintes categorias:

- Informação pública;
- Informação interna;
- Informação confidencial.

O manuseio da informação da D4Sign deverá obedecer às regras definidas para cada classificação.

O descarte da informação deve ser realizado de forma a impedir a sua recuperação, independente do seu formato de armazenamento original.

3.1.3. POLÍTICA DE CONTROLE DE ACESSO FÍSICO E DIGITAL

A D4Sign fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa e sistemas internos.

As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da D4Sign são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo.

Elaboração: Fábio Oliveira

Aprovação: Rafael Figueiredo

Revisão: 01

Data: 18/07/2025

A autorização e o nível permitido de acesso ativos/serviços de informação da D4Sign é feita com base em perfis que definem o nível de privilégio dos usuários.

Caso seja necessário acesso a algum recurso, o colaborador envia a demanda ao gestor do processo, para autorização junto ao TI.

São consideradas áreas restritas os locais onde informações de clientes são armazenadas e/ou manipuladas, em função do modelo do escritório, todas as áreas internas da empresa são consideradas restritas.

São adotadas medidas de prevenção para garantir acesso seguro:

- Após receber a senha inicial, o usuário deverá trocar a senha. As senhas são geradas preferencialmente com 12 caracteres, incluindo letras maiúsculas e minúsculas, número ou caractere especial;
- Não anotar senhas;
- Não utilizar sua conta para violar controles de segurança da informação;
- Não compartilhar contas de acesso ou senhas;

Além das práticas acima, a D4Sign possui controles internos complementares.

3.1.4. POLÍTICA DE PROTEÇÃO CONTRA AMEAÇAS E CÓDIGOS MALICIOSOS

A D4Sign disponibiliza ferramenta corporativa ESET para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de trabalho e dispositivos móveis, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, worms, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares.

Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da D4Sign devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos:

- Quando houver identificação ou suspeita de infecção ou códigos maliciosos, comunicar ao responsável pelo TI e não tentar efetuar a correção;
- Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;

Elaboração: Fábio Oliveira

Aprovação: Rafael Figueiredo

Revisão: 01

Data: 18/07/2025

- Não baixar ou instalar softwares não autorizados.

Serviços em nuvem são atualizados e monitorados continuamente, se mantendo sempre com os últimos patches de segurança.

3.1.5. POLÍTICA DE ACESSO REMOTO

O acesso remoto a ativos/serviços de informação, incluindo acesso em nuvem, e recursos computacionais da D4Sign é restrito a usuários que necessitem deste recurso para execução das atividades profissionais, como atividade de suporte ao sistema de assinaturas, assim como terceiros e prestadores de serviços.

Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto a ativos/serviços de informação ou recursos computacionais da D4Sign está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade.

O acesso poderá ser cedido a terceiros e prestadores de serviços caso seja necessário para execução de suas atividades, e devem ser seguidas tratativas de conscientização sobre questões de segurança e assinatura de termo conforme definido em políticas específicas.

3.1.6. POLÍTICA DE RESPOSTAS A INCIDENTES DE SI

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da D4Sign serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados.

Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas à D4Sign sem aprovação expressa e formal do Comitê Gestor de Segurança da Informação.

Todos os incidentes de segurança da informação ou suspeitas devem ser imediatamente comunicados à área de segurança da informação, seja por colaboradores, fornecedores, parceiros de negócios entre outros para tratativas.

Elaboração: Fábio Oliveira	Aprovação: Rafael Figueiredo	Revisão: 01 Data: 18/07/2025
----------------------------	------------------------------	---------------------------------

3.1.7. POLÍTICA DE USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO

A D4Sign fornece para seus usuários equipamentos para o desempenho de suas atividades profissionais, que devem zelar pela sua preservação. Toda manutenção e alteração de equipamento é de responsabilidade exclusiva da D4Sign. Ao final do expediente, os computadores devem ser hibernados ou desligados.

Sempre que se ausentar, deve ser acionado bloqueio de telas com senha;

Os usuários devem se atentar a engenharia social como “espiar acima do ombro”. O departamento de TI poderá, a seu critério exclusivo, permitir o uso de mídias removíveis ou com capacidade de armazenamento removível a seus colaboradores para execução de atividades profissionais, sendo o usuário responsável pela segurança física e lógica e utilização na área interna da D4Sign.

Em caso de transporte físico de mídias, é necessário que as informações sejam criptografadas.

A D4Sign disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa, sendo proibido o uso de informações no computador.

O uso de equipamentos de impressão e scanner deve ser feito exclusivamente para a impressão/reprodução/digitalização de documentos que sejam de interesse da D4Sign ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

Os usuários devem seguir como regras de segurança:

- Não deixar documentos impressos / escaneados na impressora, retirando imediatamente após uso;
- Não reaproveitar folhas já utilizadas (verso) classificadas como uso interno ou confidencial.

As instalações de processamento de informações da D4Sign serão mantidas em áreas seguras, cujo perímetro é fisicamente controlado quanto ao acesso

Elaboração: Fábio Oliveira

Aprovação: Rafael Figueiredo

Revisão: 01

Data: 18/07/2025

não autorizado, danos e quaisquer interferências de origem humana ou natural. O ambiente é monitorado através de câmeras.

Excetuando-se quando autorizados, terceiros não devem ser deixados sozinhos em áreas restritas;

Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas.

Não é permitido fumar nas dependências da D4Sign e os colaboradores devem ter atenção ao consumir qualquer tipo de alimento em suas dependências.

3.1.8. POLÍTICA DE USO DE E-MAIL E ACESSO À INTERNET

A D4Sign fornece serviços de e-mail e acesso à internet para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais.

Os serviços são continuamente monitorados, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários, tendo como objetivos proteger a organização, atestar o respeito às regras de segurança da informação da empresa, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor.

A publicação de conteúdo referente à D4Sign em mídias e redes sociais é feita pela equipe de Marketing, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização.

Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo da D4Sign sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais.

3.1.9. POLÍTICA DE PROTEÇÃO DE INFORMAÇÕES PESSOAIS EM NUVEM

A D4Sign garante que as informações recebidas para execução dos serviços prestados não serão utilizadas para nenhuma outra finalidade, e garante sua confidencialidade através de contrato de sigilo firmado com colaboradores, clientes e fornecedores. Em caso de utilização das informações para marketing, a mesma só será utilizada após o aceite formal do cliente.

Os usuários são responsáveis pela limpeza dos computadores, garantindo que os arquivos e documentos temporários sejam apagados ou destruídos.

Elaboração: Fábio Oliveira

Aprovação: Rafael Figueiredo

Revisão: 01

Data: 18/07/2025

Sempre que houver acessos não autorizados às informações e equipamentos ou instalações de processamento que resultem em perda, divulgação ou alteração de pessoal, a D4Sign comunica o cliente.

3.1.10. POLÍTICA DE USO E CONTROLE DE CRIPTOGRAFIA

A D4Sign usa a ferramenta de segurança ESET para aplicação de criptografia nos discos de máquinas Windows suportadas, assim como notebooks e mídias externas.

Os requisitos de segurança determinados pela criptografia são monitorados pela equipe de TI conforme a política.

3.1.11. POLÍTICA DE INTELIGÊNCIA ARTIFICIAL

IA, ou Inteligência Artificial, é um campo da ciência da computação que desenvolve sistemas capazes de realizar tarefas que normalmente requerem inteligência humana, como aprender, resolver problemas e tomar decisões autônomas.

A D4Sign disponibiliza recursos de inteligência artificial Gemini a seus usuários através do login do Google.

Como forma de garantir a segurança da informação na utilização dos recursos de Inteligência Artificial, é ressaltado aos colaboradores que a IA utilizará toda informação inserida como forma de aprendizado. Para isso os colaboradores são orientados nos seguintes itens: Não compartilhar informações sensíveis; Uso Adequado da ferramenta; Verificação de informações; Validação das informações; Treinamento e familiarização; Respeito às normas de propriedade intelectual;

3.1.12 POLÍTICA DE SEGURANÇA DURANTE DESENVOLVIMENTO

Está definido dentro do escopo dessa Política, as tratativas para segurança da informação durante o processo de desenvolvimento e melhorias do sistema.

Além da avaliação de risco realizada de acordo com a metodologia de avaliação de risco e tratamento de riscos, o Gestor de Tecnologia da Informação deve realizar periodicamente a avaliação dos itens:

- Os riscos relacionados a mudanças não autorizadas no ambiente de desenvolvimento;

Elaboração: Fábio Oliveira	Aprovação: Rafael Figueiredo	Revisão: 01 Data: 18/07/2025
----------------------------	------------------------------	---------------------------------

- Vulnerabilidades técnicas dos sistemas de TI utilizados no desenvolvimento;
- Atualizações de ferramentas de desenvolvimento.

Como forma de garantir a segurança do desenvolvimento e que não impacte na segurança do ambiente de operação, são realizados testes conforme descrito em **PR Garantia da Qualidade em atualizações**.

3.2. CAPACITAÇÃO E CONSCIENTIZAÇÃO

Os empregados, estagiários e terceiros autorizados devem ser capacitados para a utilização dos recursos de informação e para a aplicação dos conceitos de segurança, de forma a garantir níveis adequados de confidencialidade, integridade e disponibilidade das informações da D4Sign.

3.3. CANAL DE SUGESTÕES E DENÚNCIAS

É disponibilizado canal de denúncias e sugestões para os colaboradores e partes externas da D4Sign através do email: dpo@d4sign.com.br.

4. POLÍTICA DE SENHAS

As diretrizes de senhas da D4Sign seguem as melhores práticas de segurança da informação e estão aplicadas em todos os ambientes (internos e externos), contemplando colaboradores, prestadores de serviço e usuários da plataforma.

4.1. Regras Gerais

- As senhas são de uso pessoal e intransferível;
- Devem ser mantidas em sigilo e não podem ser compartilhadas, anotadas em locais de fácil acesso ou repassadas a terceiros;
- Sempre que receber uma senha inicial, o usuário deve alterá-la imediatamente.

4.2 Senhas de Sistemas Internos (ativos corporativos)

- Aplicam-se a contas de rede, notebooks, sistemas corporativos e demais ativos de informação sob gestão da TI;

Elaboração: Fábio Oliveira	Aprovação: Rafael Figueiredo	Revisão: 01 Data: 18/07/2025
----------------------------	------------------------------	---------------------------------

- O bloqueio automático de tela deve ser ativado quando o usuário se ausentar do equipamento;
- As senhas são geradas, preferencialmente, com 12 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais;
- Alterações periódicas podem ser exigidas conforme avaliação de risco da área de Segurança da Informação.

4.3. Senhas de Sistemas Internos não Geridos Diretamente pela TI

- Em sistemas contratados e geridos por outras áreas, as regras mínimas de segurança de senha devem seguir este Manual e demais políticas específicas, seguindo preferencialmente, com 12 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais;
- A responsabilidade primária pelo controle é da área usuária, com apoio da TI na gestão de acessos e bloqueios.

4.4. Senhas da Plataforma D4Sign (Clientes)

- As credenciais de acesso dos clientes são protegidas em conformidade com a Política de Privacidade, a Política de Proteção de Informações Pessoais em Nuvem e a Política de Controle de Acesso;
- Recomenda-se o uso de senhas robustas e, preferencialmente, a utilização de autenticação multifator (MFA);
- Dados de credenciais nunca devem ser armazenados em formato aberto; os sistemas seguem práticas de criptografia conforme a Política de Uso e Controle de Criptografia;
- As senhas criadas pelos usuários para acesso à plataforma D4Sign deverão obedecer aos seguintes critérios: exige-se, preferencialmente, o mínimo de 8 caracteres, incluindo pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial (como por exemplo !, @, #, \$).

Elaboração: Fábio Oliveira

Aprovação: Rafael Figueiredo

Revisão: 01

Data: 18/07/2025

5. GESTÃO DA SEGURANÇA

Na D4Sign a gestão da Segurança da Informação ocorre através do SGSI – Sistema de Gestão de Segurança da Informação.

O SGSI será gerenciado pelo Comitê Gestor de Segurança da Informação, CGSI.

5.1. MEMBROS DO CGSI:

Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO(CGSI), o CEO, CFO, CTO, Head de Recursos Humanos, Head de Marketing e DPO.

5.2 COMPETÊNCIAS DO CGSI:

- Difundir a cultura de Segurança da Informação;
- Propor programas de treinamento em Segurança da Informação;
- Propor projetos e iniciativas relacionados à melhoria da Segurança da Informação.

6. FORMULÁRIOS

N/A

7. GLOSSÁRIO

Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a D4Sign;

Ativo: Tudo aquilo que possui valor para a D4Sign;

Ativo de informação: Patrimônio intangível da D4Sign, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a D4Sign por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da D4Sign ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Elaboração: Fábio Oliveira

Aprovação: Rafael Figueiredo

Revisão: 01

Data: 18/07/2025

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da D4Sign, que tem por finalidade tratar questões ligadas à Segurança da Informação.

Confidencialidade: Propriedade dos ativos da informação da D4Sign, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Controle: Medida de segurança adotada pela D4Sign para o tratamento de um risco específico.

Disponibilidade: Propriedade dos ativos da informação da D4Sign, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da D4Sign.

Integridade: Propriedade dos ativos da informação da D4Sign, de serem exatos e completos.

Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação da D4Sign.

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da D4Sign.

Usuário da informação: Empregados com vínculo empregatício de qualquer área da D4Sign ou terceiros alocados na prestação de serviços a D4Sign, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar ou manipular qualquer ativo de informação da D4Sign para o desempenho de suas atividades profissionais.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da D4Sign.

Elaboração: Fábio Oliveira	Aprovação: Rafael Figueiredo	Revisão: 01 Data: 18/07/2025
----------------------------	------------------------------	---------------------------------