CRAFT.Sys
web solutions

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Diretrizes corporativas para proteção de informações, sistemas e dados

Código do documento	PSI-001
Versão	1.0
Data de emissão	05/07/2026
Data de aprovação	16/07/2026
Classificação	Uso interno e público institucional

RESPONSÁVEIS PELO DOCUMENTO

ELABORAÇÃO	APROVAÇÃO
Ana Luisa Soares Sountachi	**Fernando José de Melo Nascimento**
Advogada	CEO

CONTROLE DO DOCUMENTO

Título	Política de Segurança da Informação
Código	PSI-001
Versão	1.0
Data de emissão	05/07/2026
Data de aprovação	16/07/2026
Periodicidade de revisão	Anual ou sempre que houver alteração relevante
Responsável pela elaboração	Ana Luisa Soares Sountachi - Advogada
Responsável pela aprovação	Fernando José de Melo Nascimento - CEO

Histórico de revisões

Versão	Data	Descrição	Responsável
1.0	05/07/2026	Emissão inicial	Ana Luisa Soares Sountachi

Orientação de uso

Esta política deve ser divulgada às pessoas que tenham acesso às informações, sistemas, ambientes ou recursos tecnológicos da Craft.Sys. Procedimentos operacionais específicos poderão complementar suas diretrizes.

ÍNDICE DE SEÇÕES

1. OBJETIVO

Esta Política de Segurança da Informação estabelece os princípios, as responsabilidades e os controles adotados pela Craft.Sys para proteger suas informações, seus sistemas, códigos-fonte, ambientes tecnológicos e os dados tratados em nome de clientes, parceiros, colaboradores e fornecedores.

A política tem como objetivos:

- Preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações;
- Reduzir riscos de acessos não autorizados, vazamentos, fraudes, indisponibilidade e perda de dados;
- Estabelecer responsabilidades para o uso seguro dos recursos tecnológicos;
- Promover uma cultura de segurança da informação;
- Apoiar o cumprimento de contratos, requisitos legais e obrigações relacionadas à proteção de dados pessoais;
- Garantir a continuidade dos serviços prestados pela Craft.Sys.

2. ABRANGÊNCIA

Esta política aplica-se a:

- Sócios, diretores e colaboradores da Craft.Sys;
- Prestadores de serviços, desenvolvedores, consultores e profissionais terceirizados;
- Fornecedores que tenham acesso a informações ou ambientes da empresa;
- Sistemas desenvolvidos, administrados ou mantidos pela Craft.Sys;
- Servidores, VPS, serviços em nuvem, bancos de dados, painéis de hospedagem e ferramentas de desenvolvimento;
- Computadores, notebooks, dispositivos móveis e demais equipamentos utilizados nas atividades profissionais;
- Repositórios de código-fonte, sistemas de controle de versão e ambientes de desenvolvimento;
- Contas de e-mail, ferramentas de comunicação e plataformas colaborativas;
- Informações próprias da Craft.Sys e informações pertencentes a clientes, parceiros e usuários.

O cumprimento desta política é obrigatório para todas as pessoas que tenham acesso aos recursos tecnológicos ou às informações sob responsabilidade da Craft.Sys.

3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

3.1 Confidencialidade

As informações devem ser acessadas apenas por pessoas devidamente autorizadas e exclusivamente para finalidades profissionais legítimas.

3.2 Integridade

As informações devem permanecer completas, corretas e protegidas contra alterações indevidas, acidentais ou maliciosas.

3.3 Disponibilidade

Sistemas, dados e serviços devem estar disponíveis aos usuários autorizados conforme as necessidades operacionais e os níveis de serviço estabelecidos.

3.4 Autenticidade

A identidade de usuários, sistemas e dispositivos deve ser validada antes da concessão de acesso.

3.5 Rastreabilidade

Atividades relevantes devem ser registradas de forma que seja possível identificar acessos, alterações, falhas e eventos de segurança.

3.6 Privilégio mínimo

Cada usuário deverá possuir somente os acessos necessários para executar suas atividades.

3.7 Segurança por padrão

Novos sistemas, ambientes e funcionalidades devem ser configurados inicialmente com o nível de acesso mais restritivo possível.

3.8 Segurança desde a concepção

A segurança e a proteção de dados devem ser consideradas durante todas as etapas de planejamento, desenvolvimento, implantação e manutenção de sistemas.

4. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações tratadas pela Craft.Sys devem ser classificadas de acordo com sua sensibilidade e com os riscos relacionados ao acesso, à alteração, à divulgação ou à indisponibilidade.

4.1 Informação pública

Informação cuja divulgação não representa risco para a Craft.Sys ou para seus clientes.

- Conteúdo publicado em sites institucionais;
- Materiais comerciais aprovados;
- Informações públicas sobre produtos e serviços.

4.2 Informação interna

Informação destinada ao uso interno da Craft.Sys e que não deve ser divulgada sem autorização.

- Procedimentos operacionais;
- Comunicações internas;
- Documentação técnica não sensível;
- Informações administrativas.

4.3 Informação confidencial

Informação que pode causar prejuízo à Craft.Sys, aos clientes ou aos titulares de dados caso seja divulgada indevidamente.

- Contratos;
- Dados cadastrais de clientes;
- Informações financeiras;
- Dados pessoais;
- Documentação de infraestrutura;
- Credenciais de acesso;
- Configurações de servidores;
- Backups;
- Informações sobre vulnerabilidades.

4.4 Informação restrita

Informação de alta criticidade, cujo acesso deve ser limitado a pessoas especificamente autorizadas.

- Senhas administrativas;
- Chaves privadas;
- Tokens de APIs;
- Chaves de acesso a serviços em nuvem;
- Arquivos de configuração contendo segredos;
- Dados bancários;
- Bancos de dados de produção;
- Informações protegidas por sigilo contratual;

- Dados pessoais sensíveis.

> **Regra de compartilhamento**
> Informações confidenciais e restritas não devem ser compartilhadas por canais não autorizados. Em caso de dúvida sobre a classificação, deve ser adotado o nível mais restritivo até que o responsável confirme o enquadramento.

5. RESPONSABILIDADES

5.1 Direção da Craft.Sys

Compete à direção:

- Aprovar esta política;
- Disponibilizar recursos adequados para a segurança da informação;
- Definir responsabilidades;
- Avaliar riscos relevantes;
- Apoiar ações de prevenção, resposta e recuperação de incidentes;
- Aplicar medidas administrativas em caso de descumprimento.

5.2 Responsável pela segurança da informação

Compete ao responsável designado:

- Manter esta política atualizada;
- Avaliar vulnerabilidades e riscos;
- Coordenar a resposta a incidentes;
- Orientar colaboradores e prestadores;
- Acompanhar a aplicação dos controles de segurança;
- Recomendar melhorias técnicas e operacionais;
- Manter registros dos incidentes e das ações realizadas.

5.3 Colaboradores e prestadores de serviços

Todos os usuários são responsáveis por:

- Proteger suas credenciais;
- Utilizar os recursos exclusivamente para atividades autorizadas;
- Cumprir esta política e os procedimentos internos;
- Comunicar imediatamente incidentes ou suspeitas;
- Não instalar programas não autorizados;
- Não compartilhar informações de clientes sem autorização;
- Manter seus dispositivos protegidos e atualizados;
- Encerrar sessões e bloquear equipamentos quando estiverem sem supervisão;
- Preservar o sigilo das informações mesmo após o encerramento do vínculo com a Craft.Sys.

6. GESTÃO DE ACESSOS

Todo acesso a sistemas, servidores, bancos de dados, repositórios e ferramentas corporativas deve ser individual, autorizado e rastreável.

A concessão de acesso deverá observar:

- Necessidade profissional;
- Privilégio mínimo;
- Separação entre contas pessoais e administrativas;

- Aprovação do responsável pelo ambiente;
- Revisão periódica das permissões;
- Remoção imediata do acesso após desligamento ou término do contrato.

É proibido:

- Compartilhar usuários e senhas;
- Utilizar credenciais de outro profissional;
- Manter contas genéricas sem justificativa técnica;
- Conceder acesso administrativo quando um acesso limitado for suficiente;
- Acessar informações sem necessidade profissional;
- Tentar contornar mecanismos de autenticação ou controle de acesso.

Contas administrativas devem ser utilizadas apenas para atividades que realmente exijam privilégios elevados.

7. SENHAS E AUTENTICAÇÃO

As senhas utilizadas nos ambientes da Craft.Sys devem:

- Possuir, preferencialmente, pelo menos 12 caracteres;
- Combinar letras, números e caracteres especiais;
- Não conter informações pessoais facilmente identificáveis;
- Não ser reutilizadas em serviços pessoais ou em sistemas diferentes;
- Ser armazenadas em gerenciador de senhas aprovado;
- Ser alteradas imediatamente em caso de suspeita de comprometimento.

A autenticação multifator deverá ser ativada sempre que estiver disponível, especialmente em:

- Contas de e-mail;
- Serviços em nuvem;
- Provedores de hospedagem;
- Painéis administrativos;
- Repositórios de código;
- Sistemas financeiros;
- Contas de domínio e DNS;
- Serviços de backup;
- Ferramentas com acesso a dados de clientes.

> **Proteção de segredos**
> Senhas, tokens, chaves e segredos não devem ser enviados por e-mail, aplicativos de mensagens ou documentos sem proteção adequada. Segredos comprometidos devem ser revogados e substituídos imediatamente.

8. USO ACEITÁVEL DOS RECURSOS TECNOLÓGICOS

Os recursos tecnológicos fornecidos ou autorizados pela Craft.Sys devem ser utilizados de forma profissional, segura e responsável.

Não é permitido:

- Utilizar os recursos para atividades ilegais;
- Instalar softwares sem licença ou de origem desconhecida;
- Desativar antivírus, firewall ou mecanismos de proteção;
- Executar testes de invasão sem autorização;
- Armazenar material ofensivo, ilegal ou incompatível com as atividades profissionais;

- Utilizar ferramentas corporativas para disseminar spam, malware ou conteúdo malicioso;
- Conectar dispositivos desconhecidos a ambientes críticos;
- Compartilhar arquivos corporativos por plataformas não autorizadas;
- Utilizar dados reais de clientes em ambientes de teste sem necessidade e proteção adequadas.

A Craft.Sys poderá registrar e monitorar o uso de seus recursos tecnológicos para fins de segurança, continuidade operacional, investigação de incidentes e cumprimento de obrigações legais e contratuais.

9. SEGURANÇA DOS EQUIPAMENTOS

Computadores e dispositivos utilizados nas atividades da Craft.Sys devem possuir:

- Sistema operacional atualizado;
- Correções de segurança instaladas;
- Firewall ativo;
- Solução antimalware, quando aplicável;
- Bloqueio automático de tela;
- Senha ou autenticação biométrica;
- Criptografia de armazenamento, sempre que disponível;
- Software obtido de fontes confiáveis;
- Backup das informações necessárias à continuidade das atividades.

O usuário deve comunicar imediatamente a perda, o furto, o roubo ou o comprometimento de qualquer dispositivo utilizado para acessar recursos corporativos.

10. TRABALHO REMOTO

No trabalho remoto, os usuários devem:

- Evitar redes Wi-Fi públicas ou desconhecidas;
- Utilizar conexão segura ou VPN quando exigido;
- Manter os equipamentos sob supervisão;
- Evitar exposição de informações em locais públicos;
- Não permitir que familiares ou terceiros utilizem equipamentos corporativos;
- Utilizar somente ferramentas autorizadas;
- Proteger reuniões, documentos e telas contra visualização por terceiros;
- Manter os mesmos controles exigidos para o trabalho presencial.

11. SEGURANÇA DE SERVIDORES E INFRAESTRUTURA

Servidores, VPS, serviços em nuvem, painéis de hospedagem, contas de domínio, DNS e demais componentes de infraestrutura devem observar, sempre que tecnicamente possível:

- Atualizações regulares de sistema e aplicações;
- Restrição de portas e serviços;
- Firewall devidamente configurado;
- Acesso administrativo restrito;
- Autenticação multifator;
- Uso de chaves seguras para conexões administrativas;
- Desativação de serviços desnecessários;
- Monitoramento de logs e tentativas de acesso;
- Separação entre ambientes de desenvolvimento, homologação e produção;
- Backups periódicos;
- Certificados digitais válidos;

- Comunicação criptografada;
- Revisão periódica das contas e permissões;
- Proteção contra ataques automatizados;
- Limitação de tentativas de autenticação;
- Registro de alterações relevantes.

Sempre que possível, o acesso direto a bancos de dados e servidores de produção deve ser restrito por endereço IP, VPN ou mecanismo equivalente.

12. DESENVOLVIMENTO SEGURO DE SISTEMAS

Os sistemas desenvolvidos ou mantidos pela Craft.Sys devem observar boas práticas de desenvolvimento seguro ao longo de todo o ciclo de vida.

Devem ser considerados:

- Validação e sanitização das entradas;
- Proteção contra injeção de comandos e SQL;
- Proteção contra ataques de sessão e falsificação de requisições;
- Controle adequado de autenticação e autorização;
- Armazenamento seguro de senhas por meio de algoritmos apropriados;
- Tratamento seguro de uploads;
- Restrição de tipos e tamanhos de arquivos;
- Proteção de APIs;
- Uso de conexões criptografadas;
- Controle de erros sem exposição de informações sensíveis;
- Atualização de bibliotecas e dependências;
- Revisão de código em alterações críticas;
- Testes antes da publicação;
- Registro das alterações realizadas;
- Plano de reversão em implantações relevantes.

> **Segredos no código-fonte**
> Credenciais, senhas, tokens e chaves não devem ser gravados diretamente no código-fonte. Arquivos como .env, certificados, chaves privadas e configurações sensíveis não devem ser armazenados em repositórios públicos.

13. REPOSITÓRIOS E CÓDIGO-FONTE

O código-fonte desenvolvido pela Craft.Sys ou sob sua responsabilidade deve ser armazenado em repositórios autorizados.

Os repositórios devem possuir:

- Controle individual de acesso;
- Autenticação multifator;
- Histórico de alterações;
- Proteção das ramificações principais, quando aplicável;
- Revisão de permissões;
- Remoção de usuários inativos;
- Proibição de exposição pública sem autorização;
- Verificação para evitar o envio de credenciais e dados pessoais.

O acesso ao código-fonte de clientes deverá respeitar os contratos, as autorizações concedidas e a necessidade profissional.

14. PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais deve ocorrer somente para finalidades legítimas, específicas e compatíveis com as atividades da Craft.Sys ou com os serviços contratados pelos clientes.

Devem ser adotadas medidas para:

- Limitar a coleta ao mínimo necessário;
- Restringir o acesso aos dados;
- Manter os dados somente pelo período necessário;
- Proteger dados durante armazenamento e transmissão;
- Evitar cópias desnecessárias;
- Excluir ou anonimizar dados quando aplicável;
- Comunicar incidentes envolvendo dados pessoais;
- Atender às obrigações contratuais relacionadas à privacidade;
- Apoiar os clientes no cumprimento de suas responsabilidades, quando previsto contratualmente.

Dados pessoais não devem ser utilizados para finalidades diferentes daquelas autorizadas. A utilização de bancos de dados de produção em ambientes de teste deverá ser evitada. Quando for indispensável, os dados deverão ser reduzidos, anonimizados ou protegidos adequadamente.

15. BACKUPS

Os dados e sistemas considerados críticos devem possuir rotinas de backup compatíveis com sua importância.

Os backups devem:

- Ser realizados periodicamente;
- Ser armazenados separadamente do ambiente principal;
- Possuir proteção contra acesso não autorizado;
- Ser criptografados quando contiverem informações confidenciais;
- Ter sua execução monitorada;
- Ser submetidos a testes periódicos de restauração;
- Possuir período de retenção definido;
- Ser excluídos de forma segura após o término da retenção.

> **Validação de recuperação**
> A existência de um backup não deve ser considerada suficiente sem que sua restauração tenha sido testada e documentada.

16. GESTÃO DE FORNECEDORES

Fornecedores que tenham acesso a sistemas, infraestrutura ou informações da Craft.Sys deverão:

- Receber somente os acessos necessários;
- Cumprir requisitos de confidencialidade e segurança;
- Utilizar credenciais individuais;
- Comunicar incidentes;
- Devolver ou excluir informações ao término do contrato;
- Ter seus acessos removidos após o encerramento da atividade.

Serviços externos devem ser avaliados considerando sua finalidade, nível de segurança, criticidade e tipo de informação tratada.

17. GESTÃO DE VULNERABILIDADES E ATUALIZAÇÕES

A Craft.Sys deverá acompanhar vulnerabilidades que possam afetar seus ambientes e aplicar correções considerando a criticidade e o risco envolvido. Atualizações críticas de segurança deverão receber tratamento prioritário.

Sistemas sem suporte ou executados em versões obsoletas deverão:

- Ser atualizados;
- Ser substituídos;
- Ser isolados;
- Ou receber controles compensatórios enquanto a atualização não for possível.

Testes de segurança devem ser realizados de forma autorizada, planejada e sem comprometer a disponibilidade dos serviços.

18. REGISTRO E MONITORAMENTO

Sistemas críticos devem manter registros suficientes para auxiliar na identificação de:

- Acessos;
- Alterações administrativas;
- Tentativas de autenticação;
- Falhas;
- Erros;
- Alterações em dados;
- Atividades suspeitas;
- Incidentes de segurança.

Os registros devem ser protegidos contra alterações e acessados somente por pessoas autorizadas. O período de retenção deverá considerar a criticidade do sistema, as obrigações contratuais e as necessidades de investigação.

19. INCIDENTES DE SEGURANÇA

São exemplos de incidentes de segurança:

- Vazamento ou exposição de informações;
- Acesso não autorizado;
- Roubo de credenciais;
- Malware ou ransomware;
- Perda ou furto de equipamento;
- Exclusão ou alteração indevida de dados;
- Indisponibilidade relevante;
- Uso indevido de informações;
- Exposição de arquivos de configuração;
- Publicação de credenciais em repositórios;
- Suspeita de invasão;
- Envio de informação confidencial ao destinatário errado.

Todo incidente ou suspeita deverá ser comunicado imediatamente ao responsável designado pela Craft.Sys.

O registro deverá conter, quando possível:

- Data e horário;
- Sistema ou cliente afetado;
- Descrição do ocorrido;
- Informações possivelmente comprometidas;
- Ações já realizadas;
- Pessoas envolvidas;
- Evidências disponíveis.

> **Canal de comunicação de incidentes**
> Telefone/WhatsApp: (44) 99185-4000.

20. RESPOSTA A INCIDENTES

Ao identificar um incidente, a Craft.Sys deverá:

1. Registrar o evento;
2. Avaliar sua criticidade;
3. Conter a ameaça;
4. Preservar evidências;
5. Identificar a causa;
6. Remover o agente ou a vulnerabilidade;
7. Recuperar os serviços;
8. Validar a segurança do ambiente;
9. Comunicar as partes responsáveis;
10. Documentar as ações realizadas;
11. Implementar medidas para evitar recorrência.

A comunicação a clientes, titulares, fornecedores ou autoridades deverá ser realizada pela direção ou por pessoa formalmente autorizada. Nenhum colaborador ou prestador deverá divulgar publicamente informações sobre incidentes sem autorização.

21. CONTINUIDADE DOS SERVIÇOS

A Craft.Sys deverá manter procedimentos compatíveis com seus serviços críticos para:

- Recuperação de dados;
- Restauração de sistemas;
- Substituição de recursos tecnológicos;
- Comunicação com clientes;
- Priorização dos serviços essenciais;
- Atuação em caso de indisponibilidade;
- Recuperação após incidentes.

Os procedimentos deverão ser testados periodicamente, especialmente para serviços cuja indisponibilidade possa causar impacto relevante aos clientes.

22. DESCARTE SEGURO DE INFORMAÇÕES

Informações que não sejam mais necessárias deverão ser eliminadas de forma segura.

O descarte pode incluir:

- Exclusão segura de arquivos;
- Remoção de backups expirados;

- Destruição física de mídias;
- Revogação de tokens e chaves;
- Limpeza de equipamentos antes de sua venda ou descarte;
- Exclusão de contas e acessos;
- Remoção de dados de ambientes de teste.

Documentos impressos contendo informações confidenciais deverão ser fragmentados antes do descarte.

23. TREINAMENTO E CONSCIENTIZAÇÃO

Colaboradores e prestadores deverão receber orientações sobre:

- Proteção de credenciais;
- Reconhecimento de tentativas de fraude;
- Phishing;
- Engenharia social;
- Uso seguro de dispositivos;
- Proteção de dados pessoais;
- Comunicação de incidentes;
- Utilização segura de serviços em nuvem;
- Cuidados com códigos, bancos de dados e ambientes de produção.

Orientações adicionais poderão ser realizadas sempre que surgir uma nova ameaça ou mudança relevante nos procedimentos.

24. DESLIGAMENTO E ENCERRAMENTO DE CONTRATOS

Em caso de desligamento ou encerramento do vínculo, deverão ser adotadas as seguintes medidas:

- Revogação imediata dos acessos;
- Troca de credenciais compartilhadas que tenham sido conhecidas pelo profissional;
- Revogação de tokens, certificados e chaves;
- Recolhimento de equipamentos;
- Transferência dos arquivos e responsabilidades;
- Remoção de acessos a repositórios, servidores, e-mails e documentos;
- Confirmação da devolução ou exclusão das informações;
- Manutenção das obrigações de confidencialidade.

25. EXCEÇÕES

Qualquer exceção a esta política deverá:

- Ser justificada;
- Ser avaliada quanto aos riscos;
- Receber autorização da direção;
- Possuir prazo definido;
- Ter controles compensatórios, quando necessários;
- Ser revisada antes de sua renovação.

26. DESCUMPRIMENTO

O descumprimento desta política poderá resultar em:

- Orientação ou advertência;
- Suspensão ou remoção de acessos;

- Aplicação de medidas administrativas;
- Rescisão de contrato;
- Responsabilização por perdas e danos;
- Adoção de medidas legais cabíveis.

As medidas serão aplicadas conforme a gravidade, os impactos causados e a natureza do vínculo com a Craft.Sys.

27. REVISÃO DA POLÍTICA

Esta Política de Segurança da Informação deverá ser revisada pelo menos uma vez por ano ou sempre que houver:

- Alteração relevante na infraestrutura;
- Criação de novos produtos ou serviços;
- Mudança nos processos internos;
- Incidente relevante;
- Identificação de novos riscos;
- Alteração contratual ou regulatória;
- Mudança na estrutura da empresa.

28. APROVAÇÃO

Esta política entra em vigor na data de sua aprovação e permanece válida até a publicação de uma nova versão.

ELABORAÇÃO	APROVAÇÃO
_____	_____
Ana Luisa Soares Sountachi	**Fernando José de Melo Nascimento**
Advogada	CEO
Data: 05/07/2026	Data: 16/07/2026

TERMO DE CIÊNCIA E RESPONSABILIDADE

Declaro que recebi, li e compreendi a Política de Segurança da Informação da Craft.Sys.

Comprometo-me a cumprir as regras e os procedimentos estabelecidos, proteger as informações às quais tiver acesso e comunicar imediatamente qualquer incidente, suspeita de comprometimento ou descumprimento identificado.

Reconheço que o acesso aos sistemas e às informações da Craft.Sys e de seus clientes é concedido exclusivamente para o desempenho das minhas atividades profissionais.

Nome	
CPF	
Cargo ou função	
Empresa, quando terceirizado	
Data	____ / ____ / _____
Assinatura	

Guarda do documento

O termo assinado deve ser mantido conforme o procedimento interno de gestão documental e pelo período aplicável ao vínculo profissional ou contratual.