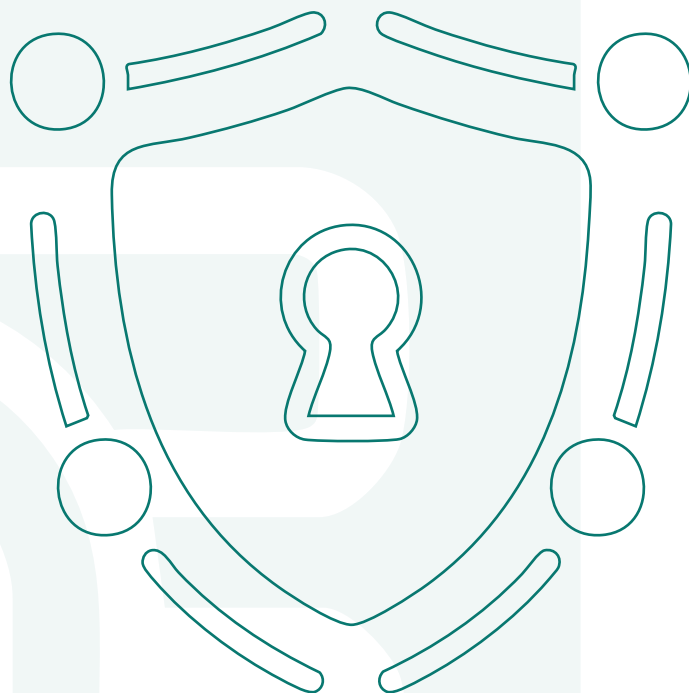




GUIA PRÁTICO EDIÇÃO 2026

PROTEÇÃO DE DADOS E SEGURANÇA DIGITAL



Linguagem simples para proteger informações,
pessoas e confiança da sociedade.



Proteção
de dados



Segurança da
informação



Responsabilidade
de todos



APRESENTAÇÃO

A transformação digital tornou os serviços públicos mais ágeis e eficientes. Ao mesmo tempo, aumentou a responsabilidade de proteger as informações utilizadas diariamente pela Administração Pública.

Na Goinfra, proteger dados pessoais significa preservar a confiança da sociedade, fortalecer a segurança da informação e contribuir para uma gestão pública mais íntegra e segura.

Este Guia Prático de Proteção de Dados e Segurança Digital – Edição 2026 foi elaborado para orientar servidores, empregados públicos, colaboradores, estagiários e demais usuários das informações institucionais.

Ao longo das próximas páginas, você encontrará orientações simples, exemplos práticos e boas práticas para proteger dados pessoais, utilizar os recursos tecnológicos com segurança e adotar comportamentos seguros no ambiente digital da Goinfra.

Mais do que cumprir normas, proteger informações é uma atitude diária.

Cada atitude faz diferença. Proteger informações é proteger as pessoas, fortalecer a Goinfra e preservar a confiança da sociedade.



SUMÁRIO

Cultura e Proteção de Dados	4
Dados Pessoais	5
Dados Sensíveis	6
Público, Restrito ou Sigiloso?	7
Quando usar Restrito ou Sigiloso no SEI?	7
Menos Acesso, Mais Proteção	9
Tela Bloqueada, Dados Seguros.....	9
Senhas Fortes, Contas Seguras	11
Atualizações e Segurança	12
Trabalho Remoto e Segurança Digital	13
Segurança Além da Tela.....	14
Dados Também Trafegam.....	16
Respeito e Responsabilidade no Ambiente Digital.....	17
Fator Humano	18
Golpes Usam Emoções	19
Engenharia Social.....	20
Pen Drive: Nem Todo Pen Drive é Seguro	22
Como verificar um pen drive antes de utilizá-lo	23
Problemas com Dados: O que Fazer?	24
Como Comunicar um Incidente	25
Antes de Compartilhar, Pergunte-se	26
Inteligência Artificial: Use com Responsabilidade	27
Armazenamento Seguro.....	28
Encerramento Seguro da Estação de Trabalho	29
Quem é a encarregada LGPD da Goinfra?	30
Direitos dos titulares dos dados pessoais.....	31
Capacitação contínua	32
Canais oficiais da Goinfra	33



CULTURA DE PROTEÇÃO DE DADOS

Proteger dados faz parte do trabalho de todos.

Na Goinfra, cada pessoa ajuda a proteger as informações da instituição. Isso acontece todos os dias, por meio de atitudes simples.

Quando você protege um documento, bloqueia o computador antes de sair ou compartilha uma informação apenas com quem precisa dela, você ajuda a evitar problemas.

Essas pequenas atitudes protegem:

- As pessoas;
- A Goinfra;
- Os serviços públicos;
- A confiança da sociedade.

A tecnologia ajuda a proteger as informações, mas a segurança também depende das atitudes de cada pessoa.

Lembre-se

Antes de acessar, compartilhar, imprimir ou descartar uma informação, faça uma pergunta:

Isso é realmente necessário?

Se a resposta for sim, faça isso com segurança.

Proteger dados é um hábito. Cada atitude faz diferença.



O QUE SÃO DADOS PESSOAIS?

Dados pessoais são informações capazes de identificar uma pessoa.

Exemplos:

- nome completo;
- CPF;
- RG;
- endereço;
- telefone;
- e-mail;
- matrícula funcional;
- fotografia;
- voz.

Regra simples

Se uma informação permite identificar uma pessoa, ela deve ser protegida.



O QUE SÃO DADOS SENSÍVEIS?

Dados sensíveis são informações que exigem proteção reforçada, pois podem expor aspectos íntimos da vida das pessoas e gerar discriminação ou prejuízos aos seus direitos.

Exemplos:

- dados referentes à saúde;
- dados biométricos;
- origem racial ou étnica;
- convicção religiosa;
- opinião política;
- filiação sindical;
- dados referentes à vida sexual;
- dados genéticos.

Importante

Essas informações merecem cuidados especiais e somente devem ser utilizadas quando houver necessidade legítima e observância da legislação aplicável.



PÚBLICO, RESTRITO OU SIGILOSO?

Nem toda informação pode ser compartilhada da mesma forma.

Antes de criar um documento no SEI, é importante verificar quem realmente precisa ter acesso ao seu conteúdo.

Algumas informações podem ser públicas. Outras precisam de acesso restrito ou até sigiloso, conforme a legislação.

Classificar corretamente um documento ajuda a proteger dados pessoais, evita o acesso indevido às informações e fortalece a segurança institucional.

Em caso de dúvida, consulte a legislação aplicável ou a área responsável antes de definir o nível de acesso.

Lembre-se:

A classificação do documento deve considerar o conteúdo da informação, e não apenas o tipo de documento.

Classificar corretamente também é proteger dados.

QUANDO USAR RESTRITO OU SIGILOSO NO SEI?

No SEI, a definição do nível de acesso deve acontecer no momento da criação do documento.

Sempre que o documento contiver dados pessoais, informações protegidas por lei ou conteúdo cujo acesso deva ser limitado, avalie se o acesso deve ser restrito ou sigiloso.

Essa decisão evita que informações sejam disponibilizadas para pessoas que não precisam conhecê-las.

Antes de concluir o cadastro do documento, confira se o nível de acesso escolhido está de acordo com o seu conteúdo.

Se o documento possuir dados pessoais ou dados sensíveis, use a classificação adequada:

Restrito

Acesso limitado aos usuários autorizados.

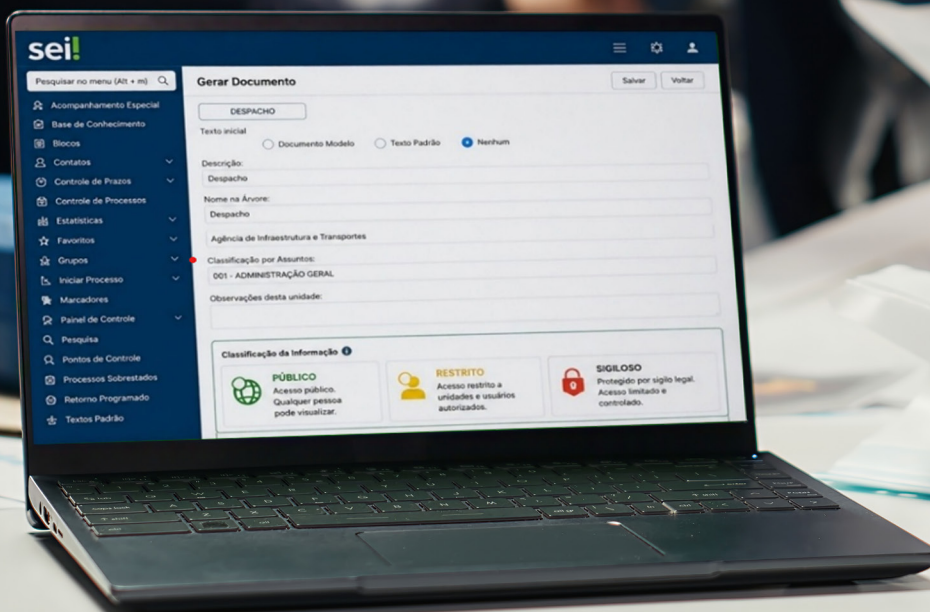
Sigiloso

Acesso protegido por previsão legal específica.

Lembre-se:

Escolher o nível de acesso correto é tão importante quanto elaborar corretamente o documento.

No SEI, proteger começa pela classificação.



MENOS ACESSO, MAIS PROTEÇÃO

Nem toda pessoa precisa acessar todas as informações.

Cada servidor deve utilizar apenas os sistemas, documentos e informações necessários para realizar suas atividades.

Esse cuidado reduz riscos, evita acessos indevidos e protege os dados da instituição.

Compartilhar senhas, utilizar contas de outras pessoas ou conceder permissões sem necessidade compromete a segurança da informação.

Sempre que um acesso deixar de ser necessário, ele deve ser revisto ou removido.

Lembre-se:

Conceder acesso apenas a quem realmente precisa protege as pessoas, a instituição e os serviços públicos.

TELA BLOQUEADA, DADOS SEGUROS

Sempre que sair da sua mesa, bloqueie a tela do computador.

Esse cuidado leva apenas alguns segundos e ajuda a proteger as informações da Goinfra.

Ao bloquear a tela, você protege:

- as informações da Goinfra;

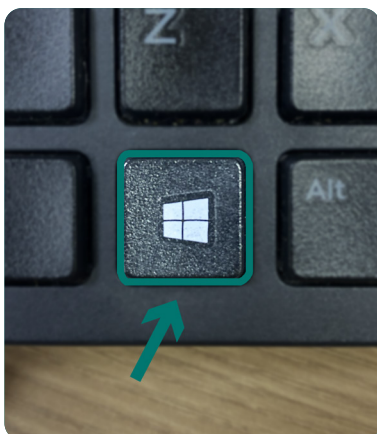
- os dados pessoais tratados pela instituição;
- os sistemas corporativos;
- sua conta de usuário.

Como bloquear a tela

Localize a tecla Windows no teclado e pressione simultaneamente:
Windows + L

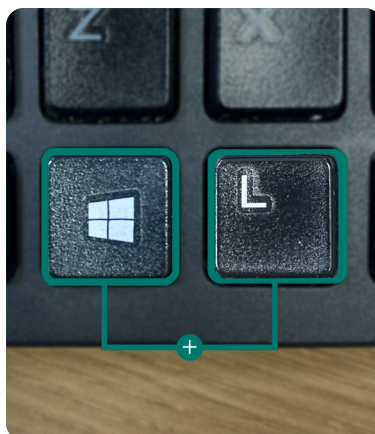
Como fazer:

Localize a tecla
Windows no teclado.



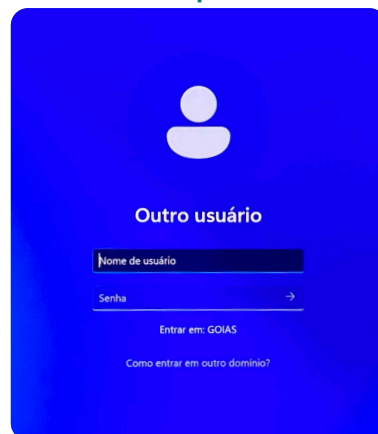
A tecla Windows normalmente fica localizada na parte inferior esquerda do teclado.

Pressione simultaneamente:
Windows + L



Pressione e mantenha pressionadas as teclas ao mesmo tempo.

Verifique se a tela
foi bloqueada.



A tela de bloqueio será exibida. Sua estação está protegida.

⚠ Importante

Criar esse hábito faz toda a diferença para manter as informações da Goinfra protegidas.

Ao retornar, basta clicar na tela, informar sua senha para continuar trabalhando normalmente.



SENHAS FORTES, CONTAS SEGURAS

A senha é a primeira barreira de proteção das suas contas e das informações da Goinfra.

Criar uma senha forte ajuda a reduzir o risco de acessos não autorizados e protege os sistemas utilizados no dia a dia.

Como criar uma senha forte:

- pelo menos 12 caracteres;
- letras maiúsculas e minúsculas;
- números;
- caracteres especiais, como `**!@#$%&***`.



⊘ Evite utilizar:

- datas de aniversário;
- nomes de familiares ou animais de estimação;
- sequências simples, como 123456 ou abcdef;
- informações pessoais fáceis de descobrir.

Lembre-se:

Nunca compartilhe sua senha com outras pessoas.

Sempre que houver suspeita de comprometimento da conta, altere a senha imediatamente.

Uma senha forte protege você, a Goinfra e as informações sob sua responsabilidade.

ATUALIZAÇÕES E SEGURANÇA

Manter os sistemas atualizados é uma das formas mais simples de proteger as informações da Goinfra.

As atualizações corrigem falhas de segurança, melhoram o funcionamento dos equipamentos e ajudam a reduzir o risco de ataques virtuais.

Boas práticas

- instale as atualizações sempre que forem disponibilizadas;
- reinicie o computador quando solicitado;
- mantenha os programas utilizados no trabalho sempre atualizados;
- utilize apenas softwares autorizados pela GOINFRA.



⛔ Evite:

- adiar atualizações por vários dias;
- instalar programas sem autorização;
- desativar recursos de segurança do computador.

Lembre-se:

Atualizar o computador é uma medida simples que ajuda a manter os sistemas mais seguros e protegidos contra novas ameaças.

Um sistema atualizado protege você, a Goinfra e as informações sob sua responsabilidade.

TRABALHO REMOTO E SEGURANÇA DIGITAL

Trabalhar fora das dependências da Goinfra exige os mesmos cuidados adotados no ambiente de trabalho.

As informações institucionais continuam protegidas, independentemente do local de acesso.

Boas práticas

- utilize apenas equipamentos autorizados ou configurados para o trabalho;
- bloqueie a tela sempre que se afastar do computador;
- mantenha seus dispositivos atualizados;
- conecte-se apenas a redes de internet confiáveis;
- proteja documentos e informações contra o acesso de pessoas não autorizadas.



🚫 Evite:

- utilizar computadores públicos ou compartilhados para acessar sistemas da Goinfra;
- deixar documentos institucionais expostos;
- compartilhar equipamentos utilizados para o trabalho com outras pessoas.

Lembre-se:

No trabalho remoto, a responsabilidade pela proteção das informações continua sendo de cada usuário.

Onde você trabalha pode mudar. O cuidado com as informações não.

SEGURANÇA ALÉM DA TELA

Muitas pessoas associam a proteção de dados apenas a computadores, sistemas e internet.

Proteger informações vai além do computador.

Na prática, a proteção de dados pessoais também se aplica a documentos físicos e informações impressas.

Documentos impressos, anotações, crachás, pen drives e outros materiais também precisam de cuidados para evitar acessos indevidos.

Boas práticas

- guarde documentos em locais seguros;
- recolha impressões imediatamente;
- mantenha a mesa organizada ao final do expediente;
- descarte documentos conforme os procedimentos da instituição;
- proteja equipamentos e mídias de armazenamento.

Lembre-se:

A proteção dos dados pessoais deve ocorrer independentemente do formato em que estejam armazenados. Na Goinfra, as informações podem estar presentes em documentos físicos, registros administrativos, sistemas eletrônicos, processos do SEI, planilhas, bancos de dados e demais ambientes institucionais.



Proteger documentos físicos também é proteger os dados da Goinfra.

DADOS TAMBÉM TRAFEGAM

As informações da Goinfra circulam todos os dias por e-mails, sistemas, aplicativos e outros meios digitais.

Antes de compartilhar qualquer informação, verifique se isso é realmente necessário e se o destinatário está autorizado a recebê-la.

Boas práticas

- confira o destinatário antes de enviar documentos;
- utilize apenas canais institucionais quando necessário;
- compartilhe somente as informações necessárias;
- confirme se o arquivo correto está sendo enviado.

❌ Evite:

- encaminhar documentos sem necessidade;
- utilizar aplicativos ou serviços não autorizados para compartilhar informações;
- enviar dados pessoais para destinatários incorretos.

Lembre-se:

Depois que uma informação é compartilhada, nem sempre é possível recuperar ou controlar sua circulação.

Dados também trafegam. Proteja cada rota.



RESPEITO E RESPONSABILIDADE NO AMBIENTE DIGITAL

O ambiente digital deve refletir os mesmos princípios de respeito, ética e responsabilidade esperados no ambiente de trabalho.

Cada usuário é responsável pelo uso adequado das informações e dos recursos tecnológicos da Goinfra.

Boas práticas

- utilize os recursos institucionais de forma responsável;
- respeite a privacidade das pessoas;
- trate as informações com sigilo quando necessário;
- comunique situações que possam colocar dados em risco.



Evite:

- acessar informações sem necessidade;
- compartilhar dados sem autorização;
- utilizar informações institucionais para fins particulares;
- divulgar conteúdos que possam comprometer a imagem da instituição.

Lembre-se:

A tecnologia ajuda a proteger as informações, mas são as atitudes das pessoas que fazem a diferença.

Respeito, responsabilidade e segurança caminham juntos.

FATOR HUMANO

A tecnologia é importante para proteger as informações, mas ela sozinha não é suficiente.

Grande parte dos incidentes ocorre por comportamento inseguro. Na maioria dos incidentes de segurança, o comportamento das pessoas faz toda a diferença.

Boas práticas

- pare e analise antes de clicar em links ou abrir arquivos;
- confirme a identidade de quem solicita informações;
- siga os procedimentos da Goinfra para proteger dados;
- utilize canais institucionais (e-mail institucional, SEI etc)
- em caso de dúvida, procure orientação;
- não deixe documentos expostos;
- bloqueie sua estação ao se ausentar;



- Evite senhas visíveis;
- Proteja informações em ambientes compartilhados.

Evite:

- e-mail pessoal;
- armazenamento privado;
- compartilhamento informal

Lembre-se:

A atenção de cada pessoa é uma das principais formas de proteger as informações da instituição.

A segurança da informação começa nas atitudes de cada usuário.

GOLPES USAM EMOÇÕES

Muitos golpes não exploram falhas nos computadores, mas sim nas emoções das pessoas.

Mensagens com urgência, promessas, ameaças ou curiosidade excessiva são utilizadas para induzir decisões rápidas e sem verificação.

Fique atento.

Desconfie de mensagens que:

- peçam informações pessoais ou senhas;
- prometam vantagens inesperadas;
- informem problemas urgentes que exigem ação imediata;
- solicitem pagamentos ou transferências;
- incentivem você a clicar em links sem confirmação.



Lembre-se:

Quando uma mensagem causar pressão, medo ou curiosidade excessiva, pare e confirme a informação antes de agir.

Na dúvida, verifique. Não tenha pressa para decidir.

ENGENHARIA SOCIAL

Engenharia social é uma técnica utilizada para convencer pessoas a fornecer informações ou realizar ações que podem comprometer a segurança.

Os criminosos utilizam manipulação psicológica e podem utilizar e-mails, mensagens, telefonemas, redes sociais ou até conversas presenciais para conquistar a confiança da vítima.

Como se proteger

- confirme a identidade de quem faz solicitações;
- nunca informe senhas ou códigos de acesso;
- não clique em links ou abra arquivos sem verificar a origem;
- comunique situações suspeitas aos canais responsáveis.

Lembre-se:

Nem toda ameaça depende de tecnologia. Muitas começam com uma simples conversa ou mensagem.



Antes de fornecer qualquer informação, pergunte-se:

Conheço quem fez a solicitação?

Essa informação realmente precisa ser compartilhada?

Posso confirmar esse pedido por outro canal oficial?

Proteger informações também significa saber dizer “não” a solicitações suspeitas.

O vazamento pode começar com um clique.



PEN DRIVE: NEM TODO PEN DRIVE É SEGURO

Um pen drive desconhecido pode conter programas maliciosos (vírus) capazes de comprometer o computador e as informações da GOINFRA. Por isso, nem todo dispositivo de armazenamento deve ser conectado aos equipamentos da instituição.

Boas práticas

- utilize apenas dispositivos autorizados;
- mantenha os arquivos protegidos;
- verifique a procedência do pen drive antes de utilizá-lo;
- siga as orientações da área de Tecnologia da Informação.

⚠ Evite:

- conectar pen drives de origem desconhecida;
- utilizar dispositivos encontrados em locais públicos;
- compartilhar mídias sem necessidade.

Lembre-se:

Um simples dispositivo pode representar um grande risco para a segurança das informações. Antes de conectar, pense. Depois de conectado, pode ser tarde.



COMO VERIFICAR UM PEN DRIVE ANTES DE UTILIZÁ-LO:

1. **Conecte o pen drive**

Conecte o dispositivo ao computador da Goinfra.

2. **Não abra nenhum arquivo**

Antes de acessar qualquer conteúdo, faça a verificação de segurança.

3. **Clique com o botão direito no pen drive**

No menu exibido, clique em “Scanear com SentinelOne”.

4. **Aguarde a verificação**

Espere o antivírus concluir a análise do dispositivo.

5. **Resultado da verificação**

Nenhuma ameaça encontrada

O pen drive pode ser utilizado normalmente.

OU

Ameaça encontrada

Não abra nenhum arquivo.

Comunique imediatamente a Gerência de Tecnologia (TI).;

PROBLEMAS COM DADOS: O QUE FAZER?

Mesmo com todos os cuidados, problemas podem acontecer. Perder um equipamento, enviar um documento para a pessoa errada ou perceber um acesso suspeito são situações que precisam ser comunicadas rapidamente.

O que fazer

- interrompa a ação, sempre que possível;
- preserve as informações relacionadas ao ocorrido;
- comunique imediatamente o fato ao canal responsável da Goinfra;
- siga as orientações recebidas.

❌ Evite:

- tentar resolver o problema sozinho;
- apagar evidências;
- deixar de comunicar o incidente por receio ou insegurança.

Lembre-se:

Comunicar rapidamente um incidente ajuda a reduzir seus impactos e protege a instituição.

Um problema comunicado rapidamente pode evitar consequências maiores.

COMO COMUNICAR UM INCIDENTE

Quando identificar ou suspeitar de um problema envolvendo informações da Goinfra, comunique o fato imediatamente pelos canais institucionais.

Quanto mais rápida for a comunicação, maiores serão as chances de reduzir os impactos e proteger os dados.

Passo a Passo

IDENTIFIQUE A SITUAÇÃO

Percebeu perda de documentos, envio incorreto de informações, acesso indevido, e-mail suspeito ou qualquer outra situação que possa comprometer dados?

INTERROMPA A AÇÃO

Sempre que possível, interrompa a atividade para evitar novos riscos.

COMUNIQUE IMEDIATAMENTE

Informe sua chefia imediata e comunique a Encarregada pelo Tratamento de Dados Pessoais ou a TI.

SIGA AS ORIENTAÇÕES

Aguarde as orientações da área responsável e colabore com a apuração do ocorrido.

AJUDE A PREVENIR NOVOS INCIDENTES

A experiência adquirida contribui para fortalecer a proteção das informações da Goinfra.



Lembre-se:

Comunicar um incidente rapidamente ajuda a proteger as pessoas, reduzir impactos e fortalecer a segurança da informação.

Comunicar também é proteger.

ANTES DE COMPARTILHAR, PERGUNTE-SE

Antes de enviar, publicar, imprimir ou compartilhar qualquer informação, faça uma rápida verificação.

Checklist

Esta informação realmente precisa ser compartilhada?

O destinatário está autorizado a recebê-la?

O canal utilizado é o mais adequado?

O documento contém dados pessoais ou informações restritas?

Estou enviando o arquivo correto?

Conferi o destinatário antes do envio?

O compartilhamento está de acordo com as normas da Goinfra?

Se alguma resposta gerar dúvida, pare e confirme antes de prosseguir.

Alguns segundos de atenção podem evitar problemas e proteger as informações da instituição.



INTELIGÊNCIA ARTIFICIAL: USE COM RESPONSABILIDADE

Ferramentas de Inteligência Artificial (IA) podem auxiliar na realização de diversas atividades. Entretanto, seu uso deve observar as normas de proteção de dados e segurança da informação da Goinfra. Nunca insira em ferramentas públicas de IA:

- processos SEI;
- documentos restritos ou sigilosos;
- contratos, pareceres e minutas;
- dados pessoais ou dados sensíveis;
- planilhas e bases de dados institucionais;
- informações estratégicas;
- senhas, credenciais ou qualquer informação institucional não pública.

A IA pode ser utilizada para:

- revisar textos sem informações institucionais;
- corrigir ortografia;
- melhorar a redação;
- resumir conteúdos públicos;
- organizar ideias.

Atenção

Sempre considere que as informações inseridas em ferramentas públicas de Inteligência Artificial podem ser processadas em ambientes externos à Goinfra.

Quando a Goinfra ou o Estado de Goiás disponibilizar ferramenta institucional de Inteligência Artificial, utilize preferencialmente essa solução, observando as orientações da área de Tecnologia da Informação e as normas internas de segurança da informação.

Na dúvida, não compartilhe informações institucionais, e procure orientação da área competente.

Proteger informações também significa utilizar a Inteligência Artificial de forma responsável.

ARMAZENAMENTO SEGURO

As informações produzidas ou utilizadas pela Goinfra devem permanecer armazenadas somente em ambientes autorizados pela instituição.

Sempre que possível, utilize:

- sistema Eletrônico de Informações (SEI);
- rede corporativa da Goinfra;
- oneDrive corporativo, quando disponibilizado pela instituição;
- sharePoint institucional, quando disponibilizado;
- servidores institucionais;
- outros ambientes autorizados pela TI.

Evite armazenar documentos institucionais em:

- google Drive pessoal;
- oneDrive pessoal;
- dropbox;
- iCloud;



- box;
- mega;
- HDs externos;
- SSDs portáteis;
- pen drives particulares;
- outros serviços ou dispositivos não autorizados.

Armazenar corretamente as informações também é proteger os dados da Goinfra.

ENCERRAMENTO SEGURO DA ESTAÇÃO DE TRABALHO

Ao final do expediente, desligue completamente o computador, salvo quando houver orientação diferente da área de Tecnologia da Informação.

Bloquear a tela protege o computador durante ausências temporárias. Ao encerrar o trabalho, desligar o equipamento reduz riscos e contribui para a segurança das informações da Goinfra.

Antes de sair:

- salve seus arquivos;
- feche todos os sistemas;
- remova pen drives, HDs externos e outros dispositivos utilizados;
- encerre conexões remotas, quando houver;
- desligue completamente o computador.

Desligar o computador ao final do expediente também é uma medida de segurança da informação.

QUEM É A ENCARREGADA LGPD DA GOINFRA?

A Encarregada pelo Tratamento de Dados Pessoais atua como canal de comunicação entre:

- a Goinfra;
- os titulares dos dados;
- a Autoridade Nacional de Proteção de Dados – ANPD.

Também auxilia:

- na orientação sobre proteção de dados;
- na disseminação de boas práticas;
- nas ações de conscientização;
- no fortalecimento da governança de proteção de dados

ENCARREGADA PELO TRATAMENTO DE DADOS PESSOAIS

Silvana Marques de Mattos

Técnico em Gestão Pública

Assessora da Diretoria de Gestão Integrada

Designada pela Portaria Goinfra n.º 88, de 19 de maio de 2026 (SEI n.º 90655202).

Contato institucional:

encarregado.goinfra@goias.gov.br / 62 3265-4209

DIREITOS DOS TITULARES DOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados (LGPD) garante diversos direitos às pessoas cujos dados pessoais são tratados pelas organizações.

Entre eles:

- acesso aos dados pessoais;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados, quando aplicável;
- eliminação de dados em situações previstas na legislação;
- oposição ao tratamento de dados em casos específicos;
- revisão de decisões tomadas exclusivamente por tratamento automatizado;
- obtenção de informações sobre a utilização dos seus dados pessoais.

Na prática, toda pessoa tem o direito de:

- solicitar informações sobre seus dados pessoais;
- pedir correção de informações incorretas;
- conhecer como seus dados são utilizados;
- solicitar esclarecimentos sobre o tratamento realizado pela Administração Pública.



A proteção da privacidade fortalece a confiança entre as pessoas e a Administração Pública.



CAPACITAÇÃO CONTÍNUA

A proteção de dados pessoais e a segurança da informação exigem atualização constante.

A Goinfra incentiva a participação em ações de capacitação relacionadas a:

- LGPD;
- Segurança da Informação;
- Compliance Público;
- Governança Digital;

Onde buscar capacitação?

- **ENAP – Escola Nacional de Administração Pública**

Disponibiliza cursos gratuitos sobre LGPD, Governança, Integridade, Transformação Digital e Gestão Pública.

- **EGOV – Escola de Governo de Goiás**

Disponibiliza cursos voltados à Administração Pública Estadual, Segurança da Informação, Compliance Público, Integridade, Gestão de Riscos e temas institucionais.

- **Plano de Capacitação da Goinfra**

Disponibiliza ações de desenvolvimento e capacitação voltadas aos servidores da Agência.

A capacitação contínua fortalece a cultura de proteção de dados, reduz riscos e contribui para serviços públicos mais seguros e confiáveis.

CANAIS OFICIAIS GOINFRA

Utilize sempre os canais institucionais para tratar assuntos relacionados à proteção de dados pessoais e à segurança da informação.

Portal LGPD Goinfra

<https://www.goinfra.go.gov.br/LGPD/330>

Portal do Servidor (Intranet GOINFRA)

Acesse documentos, normas e orientações institucionais relacionados à proteção de dados e à segurança da informação, incluindo:

- Guia Prático de Proteção de Dados e Segurança Digital;
- Política de Segurança da Informação – PLT.003;
- materiais de capacitação;
- normativos, orientações e conteúdos institucionais.

⚠ Evite utilizar canais informais para compartilhar informações institucionais ou dados pessoais.

Utilize sempre os canais oficiais da Goinfra.

COMPROMISSO INSTITUCIONAL

A proteção de dados pessoais é parte essencial da segurança institucional, da governança pública e da confiança da sociedade.

A construção de um ambiente seguro depende da atuação responsável de gestores, servidores, colaboradores e parceiros institucionais.

**DADOS TAMBÉM TRAFEGAM.
PROTEJA CADA ROTA.**

Cuidar da informação é cuidar da própria GOINFRA.

Guia Prático de Proteção de Dados e Segurança Digital
Edição 2026

Agência Goiana de Infraestrutura e Transportes
Secretaria de Estado da Infraestrutura
Governo do Estado de Goiás