

Uso Seguro e Responsável da IA

Lucimara Desiderá, M.Sc.

**Analista de Segurança
CERT.br/NIC.br**

**SEGINF2026 - Semana de Segurança da Informação da ITAIPU Binacional
Foz do Iguaçu, PR – 17 de setembro de 2026**

cert.br nic.br cgi.br

TLP:CLEAR

Núcleo de Informação e Coordenação do Ponto BR – NIC.br

Pessoa jurídica de direito privado, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

Dentre seus objetivos estão:

- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- **atender aos requisitos de segurança e emergências na Internet Brasileira em articulação e cooperação com as entidades e os órgãos responsáveis, atividades do CERT.br;**
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br;
- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.

<https://www.nic.br/sobre/>

<https://www.nic.br/estatuto-nic-br/>

Membros e ex-membros do CGI.br
(somente os atuais membros tem direito a voto)



Assembleia Geral

7 membros eleitos
pela Assembleia Geral



Conselho de Administração



Conselho Fiscal

- Administração
- Jurídico
- Comunicação
- Assessorias:
CGI.br, Políticas Públicas Digitais e Presidência
- Desenvolvimento de
Sistemas Web



Diretoria Executiva

1. Diretor presidente
2. Diretor administrativo e financeiro
3. Diretor de serviços e tecnologia
4. Diretor de projetos especiais e de desenvolvimento
5. Diretor de assessoria às atividades do CGI.br

registro.br

Domínios

cert.br

Segurança

cetic.br

Indicadores

ceptro.br

Redes e
Operações

ceweb.br

Tecnologias
Web

ix.br

Troca de
Tráfego



Observatório
de IA

ceregi.br

Centro de
Referência

Serviços Prestados à Comunidade

Gestão de Incidentes

- ▶ Coordenação
- ▶ Análise Técnica
- ▶ Suporte à Mitigação e Recuperação

Consciência Situacional

- ▶ Aquisição de Dados
 - ▶ *Honeypots* Distribuídos
 - ▶ SpamPots
 - ▶ *Threat feeds*
- ▶ Compartilhamento das Informações

Transferência de Conhecimento

- ▶ Conscientização
 - ▶ Desenvolvimento de Boas Práticas
 - ▶ Cooperação, Eventos e Reuniões (*Outreach*)
- ▶ Treinamento
- ▶ Aconselhamento Técnico e de Políticas

Filiações e Parcerias:



SEI
Partner
Network



<https://cert.br/sobre/> | <https://cert.br/sobre/filiacoes/> | <https://cert.br/about/rfc2350/>

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
 - Ponto de contato nacional de último recurso
 - Trabalho colaborativo com outras entidades
 - Auxílio na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Desmistificando a IA

Desmistificando a IA

Entendendo as Limitações

Não existe uma IA geral que faça tudo

- são **vários tipos** com **fins específicos**
- **todos tem limitações**

IA mais usada atualmente: **Grandes Modelos de Linguagem (LLMs)**

- **Não "sabe" a resposta certa**
 - calcula a **resposta mais provável**
- **Depende dos dados** de treinamento
 - **dados ruins, respostas ruins**
- É programada para **sempre dar uma resposta**
 - **mesmo que errada**

Privacidade e Proteção de Dados

Privacidade e Proteção de Dados

Tudo Vai Para os Servidores da IA

O que você **insere** no *chatbot* geralmente **vai** para a empresa que mantém a IA

- pode ser usado para:
 - **melhorar o modelo**
 - **criar perfil** sobre você
- pode **aparecer em respostas** para outras pessoas
- **Assuma que o que vai para a IA é público**
 - "Eu colocaria essa informação em um cartaz na rua?"



Privacidade e Proteção de Dados

Atenção a Configurações e ao *Prompt*

- **Ajuste configurações de privacidade**
 - **desative** o uso de suas interações para melhorar o modelo
 - **desligue o histórico** de atividade
 - use *chat* temporário ou modo incógnito, se disponível
- **Não inclua dados sensíveis no *prompt***
 - **troque** dados sensíveis por **termos genéricos**, como:
 - "nome", "CPF", "senha", "empresa", "cliente"

Cuidados com *Prompts* e Alucinações

Cuidados com *Prompts* e Alucinações

Instruções, Contexto e Fontes de Informações

Chatbots são, em essência, **geradores de texto**

- **sem contexto**, podem gerar **respostas erradas ou sem fundamento real**

- **Elabore *prompts* com contexto**

- **descreva a tarefa** a ser realizada

- indique o que espera como resultado

- **explique o contexto**

- a situação ou o cenário, condições, público-alvo e formato desejado

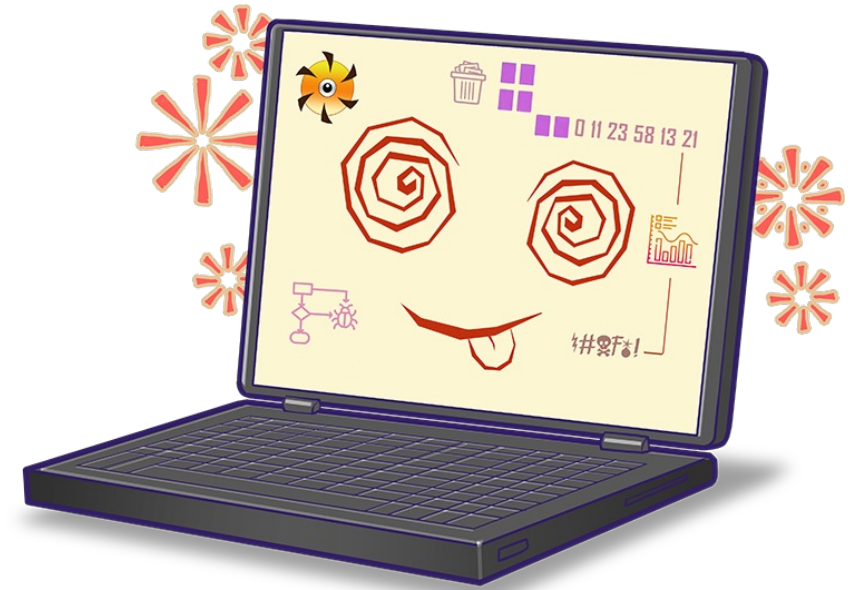
- **Forneça fontes especializadas para temas específicos**

- inclua a fonte no *prompt* e **limite a resposta a ela**

- peça trechos da fonte para validar a resposta

- **Instrua a IA a responder que não sabe**

- ex: "Se faltar informação ou não tiver certeza, diga que não sabe."



Tratando as Respostas da IA

Tratando as Respostas da IA

Valide as Informações

Usar as respostas da IA sem checar pode levar a:

- decisões erradas
 - perdas financeiras
 - danos à imagem
 - riscos à saúde
-
- Trate a resposta como um **rascunho a ser corrigido**
 - Peça à IA que **cite as fontes das informações**
 - **cheque** se são reais e se tratam do assunto
 - **Valide as informações em outras fontes**
 - se os dados e fatos estão corretos
 - se as informações estão atualizadas



Tratando as Respostas da IA

Remova Informações Sensíveis da Resposta

As respostas da IA podem conter informações sensíveis

– ex: *prompt* original, senhas ou outros dados sensíveis

– **Examine** a resposta **além do conteúdo principal**

– ex: **metadados** de arquivos, **comentários** de código

– **Remova** as informações que **não devem ser divulgadas**

Agentes de IA

Agentes de IA

Restrinja Permissões e Autonomia

Agentes de IA podem:

- **interpretar mal** instruções ou **agir de forma inesperada**
- **ser manipulados** por instruções escondidas (***prompt injection***)

Permissões e acessos **excessivos** podem levar a

- **vazamentos de dados**
- **prejuízos**

- **Limite o acesso** de agentes a informações
 - **Não forneça informações sensíveis**, como senhas e dados bancários
 - **digite** você mesmo, **quando necessário**
 - Defina uma **pasta de trabalho** para cada agente
 - **não grave informações sensíveis** nesta pasta

Agentes de IA

Restrinja Permissões e Autonomia

- **Restrinja as permissões** dos agentes
 - **autorize só o necessário** para realizar a tarefa
 - ex: não permita escrita se o agente só precisa ler
 - **não deixe** que o agente **acesse todo o sistema**
 - defina uma pasta de trabalho
- **Limite** o que agentes podem **decidir sozinhos**
 - Configure-os para **exigir sua aprovação** antes de:
 - efetivar transações financeiras
 - usar informações sensíveis
 - enviar mensagens ou publicar conteúdo em seu nome
 - executar **ações que não podem ser desfeitas**

IA na Vida Profissional

IA na Vida Profissional

Respeite a Política da Empresa

Usar IA para **processar informações internas** pode levar ao **vazamento de informações** confidenciais.

- ex: como códigos-fonte de *software*, atas de reuniões, dados de clientes

- Antes de usar IA no trabalho, **informe-se** sobre:
 - **quais ferramentas** podem ou não ser usadas
 - quais **usos** são **permitidos e proibidos**
 - **como lidar com informações sensíveis**
- **Não use contas pessoais para tarefas do trabalho**

IA na Vida Profissional

Evite Plágio

Modelos são **treinados** com **imensos volumes de textos** incluindo obras protegidas por direitos autorais. Podem **reproduzir** trechos dessas obras **sem citar a fonte**, o que pode resultar em **plágio**.

- Evite o Plágio
 - revise e **reescreva** o texto da IA **com suas próprias palavras**
 - **cite a fonte e a autoria** ao usar trabalhos de outras pessoas
 - indique **onde IA foi usada e com que objetivo**
 - lembre-se: **no final, você é o responsável!**



Golpes e Fraudes Usando IA

Golpes e Fraudes Usando IA

Desconfie de Imagens, Áudios e Vídeos

Golpistas usam IA para **criar *deepfakes***. Eles **fingem ser alguém conhecido ou famoso para pedir dinheiro, fazer propaganda enganosa ou espalhar informações falsas.**

- Antes de acreditar, **pergunte-se**:
 - essa pessoa realmente diria isso?
 - envolve dinheiro, vantagem ou dados pessoais?
 - há urgência, ameaça ou apelo emocional?
- Use verificadores de conteúdo feito por IA
 - algumas empresas oferecem recursos para verificar conteúdos gerados por suas ferramentas
- Na dúvida, **considere que é falso**



Golpes e Fraudes Usando IA

Suspeito de Comprovantes Digitais

Golpistas usam IA para **gerar imagens falsas**, como **comprovantes** de transferência e de encomendas despachadas para **fraudar consumidores**.

- Ao fazer compras:
 - **faça todo o processo** pela **plataforma oficial**
 - **confira o valor e os dados do recebedor** antes de concluir o pagamento
 - **denuncie** cobranças recebidas por outros canais
- Ao receber um comprovante de pagamento, **confira o crédito em sua conta**

IA e Saúde

Não Troque Profissional de Saúde Por IA

Chatbots de uso geral **não têm treino específico** e usam informações **nem sempre confiáveis**.

- **podem dar respostas erradas ou prejudiciais**
 - podem gerar pânico ou ilusão de normalidade
 - são incapazes de atuar em emergências
 - não consideraram o contexto do paciente
-
- **Não tente se autodiagnosticar ou automedicar**
-
- **Não faça da IA um terapeuta.** Ela:
 - não tem consciência, nem emoção e **não "entende" você**
 - tende a concordar, podendo **reforçar ideias** negativas
-
- Lembre-se: em interações com IA **não há sigilo profissional**



Checklist e Saiba Mais

Checklist

...

Tirou as informações sensíveis do prompt?



...

Checou a resposta?



...

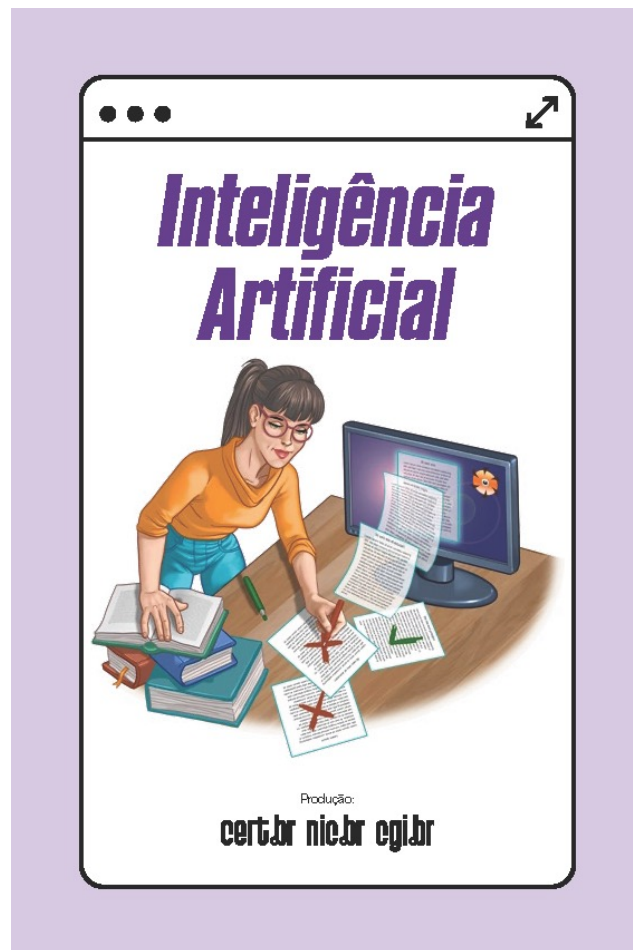
Limitou as ações dos agentes?



**IA É
ASSISTENTE.
O RESPONSÁVEL
É VOCÊ!**

Cartilha de Segurança para Internet Fascículos – Versões Digital e Impressão

Cartilha de Segurança
para Internet



<https://cartilha.cert.br/>

Conscientização de Todos é Essencial: Portal InternetSegura.br

Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!

CONFIRA A NOVIDADE!



para Crianças

CONFIRA A NOVIDADE!



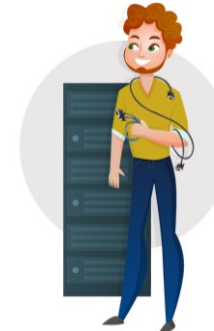
para Adolescentes



para Pais e Educadores



para 60+



para Técnicos

CONFIRA A NOVIDADE!



para Interesse Geral

<https://internetsegura.br/>

Redes Sociais

Perfil @InternetSeguraBR



<https://instagram.com/InternetSeguraBR/>

TLP:CLEAR

cert.br nic.br cgi.br

Obrigada!

© para materiais de conscientização: doc@cert.br

© notificações para: cert@cert.br

X @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br

TLP:CLEAR