VI SEMANA DE SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO

Microsoft 365 Copilot com segurança e governança

IA generativa no dia a dia da CAPES: produtiva, protegida e sob controle da instituição.

Identidade | Permissões | Proteção de dados | Governança | Pessoas

Adilson Santos
Microsoft Elevate · Sr Digital Specialist
Workshop de Inteligência Artificial (Copilot) · 05/11/2026

Segurança começa em você.
Proteção se constrói com todos.

MICROSOFT 365 COPILOT · SEGURANÇA E GOVERNANÇA

IA que trabalha dentro das regras da CAPES

O Copilot não abre um caminho novo até os dados. Ele usa as mesmas identidades, permissões e políticas que já protegem o seu Microsoft 365.

Só vê o que você já pode ver

Respeita as permissões de arquivos, sites, e-mails e chats. Não há acesso extra.

Seus dados não treinam a IA

Prompts, respostas e documentos da CAPES não são usados para treinar os modelos de linguagem.

Mesmos compromissos do Microsoft 365

Mesmos termos contratuais do e-mail e dos arquivos, com dados criptografados em trânsito e em repouso.

A IA herda as regras da instituição. Ela não cria atalhos.

POR DENTRO DE CADA PERGUNTA

Do login à resposta: 5 camadas de proteção

01
Identidade
O Entra ID confirma quem é você, com MFA e Acesso Condicional, antes de qualquer prompt.

02
Prompt protegido
Classificadores barram tentativas de jailbreak e de injeção de prompt.

03
Permissões
O Microsoft Graph só entrega o conteúdo a que você já tem acesso.

04
Rótulos
Respeita rótulos de sensibilidade e criptografia. O conteúdo gerado herda o rótulo mais restritivo.

05
Registro
A interação fica auditável no Microsoft Purview, com auditoria, retenção e eDiscovery.

A identidade é a nova fronteira da defesa.
Sem MFA forte e Acesso Condicional, as camadas seguintes perdem a força.

GOVERNANÇA PARA A DTI

O que a TI controla antes, durante e depois

Antes preparar o terreno

- **Relatórios de compartilhamento excessivo** e revisões de acesso a sites (SharePoint Advanced Management)
- **Restricted Content Discovery:** tira sites sensíveis do alcance do Copilot
- **Rótulos de sensibilidade** nos acervos críticos

Durante proteger o uso

- **DLP para o Copilot:** impede que conteúdos com determinados rótulos sejam processados
- **Acesso Condicional** específico para o Copilot
- **Controles de administração:** pesquisa na web, agentes permitidos e quem usa

Depois comprovar e responder

- **Auditoria** de cada interação com o Copilot
- **Retenção e eDiscovery** de prompts e respostas
- **DSPM para IA:** painel de riscos e uso de IA na organização

i Alguns recursos dependem do licenciamento contratado. Podemos mapear com a DTI o que a CAPES já tem disponível.

Governança não freia a IA. É ela que permite escalar o uso com confiança.

CENÁRIO ILUSTRATIVO

O risco real é o compartilhamento excessivo, e ele tem solução

A SITUAÇÃO

Uma planilha com dados de bolsistas ficou aberta para “Todos da organização”

Ela tem CPF e dados bancários, que são dados pessoais protegidos pela LGPD.

LGPD | Link amplo

SEM GOVERNANÇA

A planilha pode aparecer numa resposta do Copilot

Um servidor pergunta sobre pagamentos de bolsas. Como o acesso já existia, o Copilot pode usar a planilha.

COM GOVERNANÇA

O conteúdo fica protegido e o problema é corrigido na origem

O rótulo “Restrito” e a DLP para o Copilot impedem o uso do conteúdo. O relatório de compartilhamento aponta o link amplo e o responsável corrige.

O Copilot não cria vazamentos. Ele expõe permissões que já estavam abertas.

Por isso, revisar os acessos é o primeiro passo de qualquer implantação.

RESPONSABILIDADE COMPARTILHADA

6 hábitos para usar o Copilot com segurança

1 Use a conta institucional

Entre com o login da CAPES e confira o ícone de proteção de dados no Copilot.

2 Nada sigiloso em IA pública

Dados da CAPES só em ferramentas aprovadas pela DTI.

3 Classifique o que você cria

Aplique o rótulo de sensibilidade correto aos seus documentos.

4 Revise antes de usar

Confira as citações e as fontes. A responsabilidade final é sua.

5 Compartilhe o mínimo

Prefira links para pessoas específicas, não para toda a organização.

6 Desconfie e reporte

Instrução estranha ou pedido urgente? Confirme e avise a DTI.

Microsoft	DTI da CAPES	Você
protege a plataforma	governa o ambiente	usa com consciência

PRÓXIMOS PASSOS

Roteiro para uma adoção segura na CAPES

01

Preparar

Mapear e corrigir o compartilhamento excessivo; revisar permissões de sites e equipes.

02

Proteger

Publicar rótulos de sensibilidade, DLP para o Copilot e Acesso Condicional.

03

Capacitar

Piloto com casos de uso prioritários e trilha de capacitação para os servidores.

04

Monitorar

Auditoria, relatórios de uso e ajuste contínuo das políticas.

Segurança começa em você.

Proteção se constrói com todos: Microsoft, DTI e cada servidor.

Obrigado! Perguntas?

Adilson Santos · Microsoft Elevate
adsantos@microsoft.com