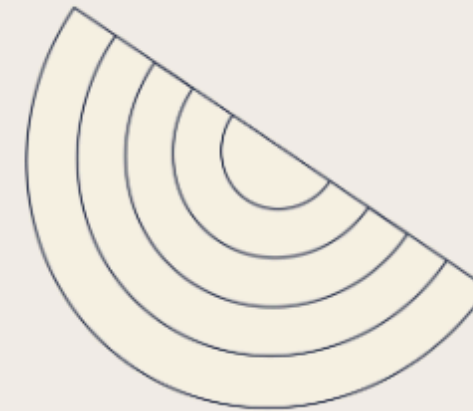




Guia PGD: Segurança da Informação

Boas práticas de segurança da
informação no Teletrabalho





Segurança da Informação

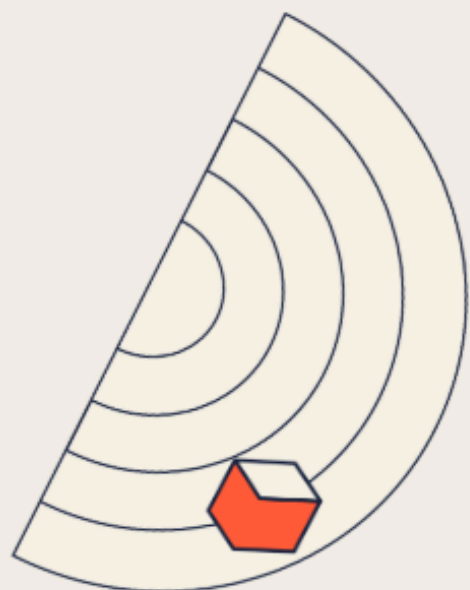


A segurança da informação tem como objetivo garantir a **confidencialidade**, **integridade**, **disponibilidade** e **autenticidade** das informações, por meio da adoção de controles que reduzam riscos e minimizem os impactos de incidentes de segurança. Para isso, é necessário identificar e mitigar vulnerabilidades que possam ser exploradas por ameaças.



Além da proteção das informações, as normas internacionais também destacam a importância da **privacidade dos dados pessoais**, estabelecendo princípios e diretrizes para seu tratamento seguro em sistemas de tecnologia da informação.

Nesse contexto, a **conscientização dos usuários** é uma das medidas mais eficazes para fortalecer a segurança da informação, contribuindo para a redução de vulnerabilidades e para a proteção dos dados institucionais e pessoais.





Princípios de segurança da informação e responsabilidades no teletrabalho





Os 4 pilares da Segurança da Informação



Confidencialidade

A confidencialidade garante que as informações sejam acessadas apenas por pessoas autorizadas. Em outras palavras, cada pessoa deve ter acesso somente aos dados necessários para realizar suas atividades.

Esse princípio pode ser comprometido quando informações são compartilhadas indevidamente, expostas em locais públicos ou acessadas por pessoas sem autorização.



Integridade

A integridade garante que as informações permaneçam corretas, completas e sem alterações indevidas durante todo o seu ciclo de vida, seja quando estão armazenadas ou sendo transmitidas.

Esse princípio pode ser comprometido quando dados são modificados sem autorização, armazenados em locais inseguros ou transmitidos por canais não protegidos.

Disponibilidade

A disponibilidade garante que as informações e os sistemas estejam acessíveis às pessoas autorizadas sempre que necessário para a realização de suas atividades.

Esse princípio pode ser comprometido por falhas técnicas, indisponibilidade de sistemas, perda de arquivos ou armazenamento inadequado das informações.



Autenticidade

A autenticidade garante que uma informação, ação ou comunicação possa ser associada de forma confiável à pessoa, sistema ou instituição que realmente a realizou.

Para isso, é fundamental que cada usuário utilize suas próprias credenciais de acesso e adote boas práticas de segurança para proteger sua identidade digital.





Privacidade

A privacidade está relacionada à proteção dos dados pessoais e ao respeito aos direitos dos titulares dessas informações. Seu objetivo é garantir que os dados sejam coletados, utilizados, compartilhados e armazenados de forma adequada, segura e transparente.

A privacidade pode ser comprometida quando dados pessoais são acessados, compartilhados ou utilizados sem necessidade, autorização ou finalidade legítima.

Como contribuir: Trate apenas os dados pessoais necessários para suas atividades, compartilhe informações com responsabilidade e siga as normas institucionais de proteção de dados.

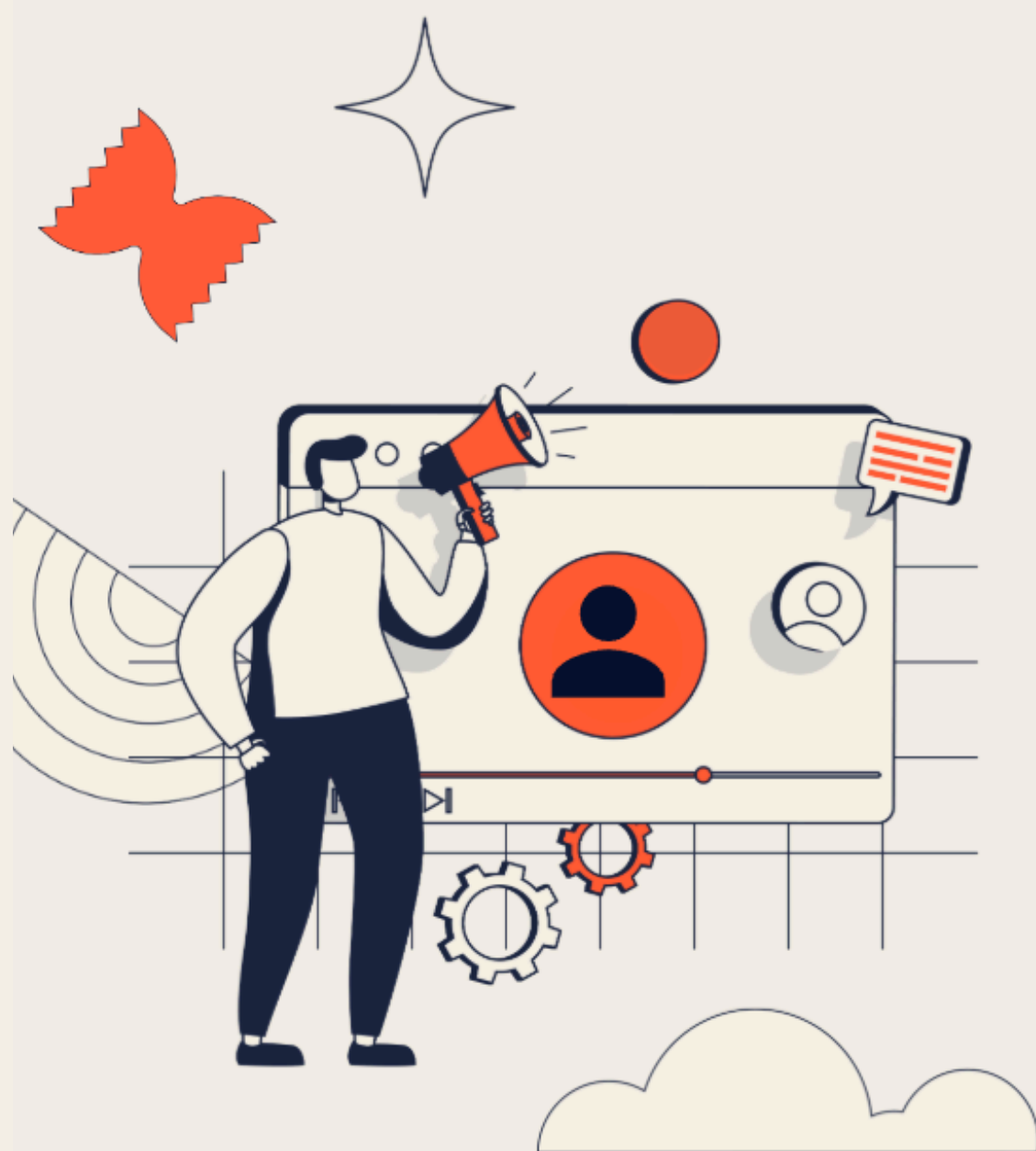
Lembre-se: proteger a privacidade significa respeitar as pessoas por trás dos dados, garantindo que suas informações sejam utilizadas de forma segura, ética e adequada.





Adoção de práticas seguras no PGD

PGD com foco em segurança e conformidade institucional



SUA RESPONSABILIDADE NO PGD

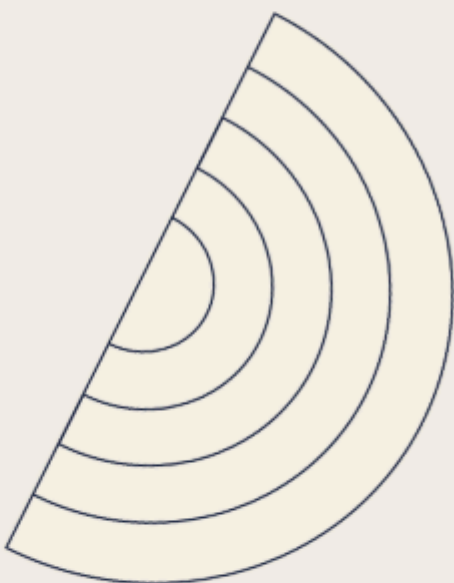
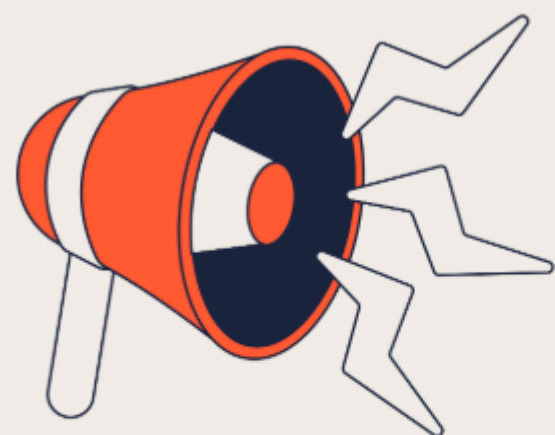
Ao aderir ao PGD, o participante deve:

- ✓ providenciar a estrutura física e tecnológica necessária ao teletrabalho;
- ✓ observar as orientações de segurança da informação estabelecidas pela UFCG;
- ✓ utilizar os recursos tecnológicos de forma segura;
- ✓ preservar o sigilo das informações institucionais;
- ✓ proteger os dados pessoais tratados durante a execução de suas atividades;
- ✓ comunicar imediatamente qualquer incidente de segurança.



ACESSO SEGURO AOS SISTEMAS DA UFCG

Teletrabalho exige atenção permanente à segurança dos dados e proteção das informações institucionais



- Utilize exclusivamente suas credenciais institucionais;
- Mantenha suas senhas em sigilo;
- Ative a autenticação em dois fatores quando disponível;
- Bloqueie a tela ao se ausentar do computador;
- Utilize apenas sistemas e plataformas autorizados pela UFCG;
- Mantenha seu sistema operacional e aplicativos atualizados.



- Nunca compartilhe sua senha;
- Não permita que terceiros utilizem sua conta institucional;
- Não salve senhas em papéis ou arquivos desprotegidos;
- Não utilize contas pessoais para armazenar documentos institucionais.





SENHAS SEGURAS

Uma senha forte deve possuir:

- ✓ letras maiúsculas;
- ✓ letras minúsculas;
- ✓ números;
- ✓ caracteres especiais;
- ✓ tamanho adequado.

Exemplo:

✗ ufcg123

✗ julho2026

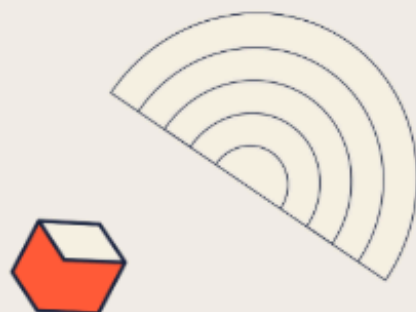
✓ Pgd!Ufcg#2026@Seg



COMPUTADOR E DISPOSITIVOS

Antes de iniciar suas atividades, verifique:

- Sistema operacional atualizado;
- Navegador atualizado;
- Antivírus instalado e atualizado;
- Firewall habilitado;
- Bloqueio automático de tela ativado;
- Backup das informações realizado regularmente.



CELULARES

Devido aos diversos sistemas acessíveis pelo aparelho celular, bem como às várias informações existentes nesses dispositivos móveis, em caso de **roubo, furto ou perda do celular**, é importante registrar um boletim de ocorrência e solicitar à operadora o bloqueio da linha e do aparelho, evitando o uso indevido do dispositivo e possíveis prejuízos. Também é recomendado comunicar o ocorrido à chefia imediata e às equipes com as quais você trabalha.

Os smartphones modernos oferecem recursos de **localização, bloqueio remoto e apagamento de dados**, permitindo proteger informações pessoais e institucionais armazenadas no aparelho. Essas funcionalidades devem ser utilizadas sempre que possível para preservar a segurança e a privacidade dos dados.



Boas práticas operacionais e proteção contra golpes





Uso de Wi-Fi com preferências seguras e evitações

Prefira rede residencial protegida por senha

Rede residencial protegida por senha é recomendada para acessar sistemas institucionais.

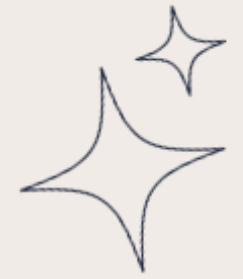
Use VPN institucional quando disponível

Utilize a VPN institucional, quando disponível.

Evite Wi-Fi público de cafeterias aeroportos e hotéis

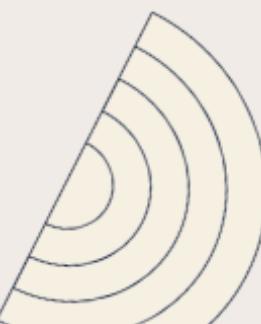
Evite Wi-Fi de cafeterias, aeroportos, hotéis e redes públicas abertas.

Cuidados com phishing

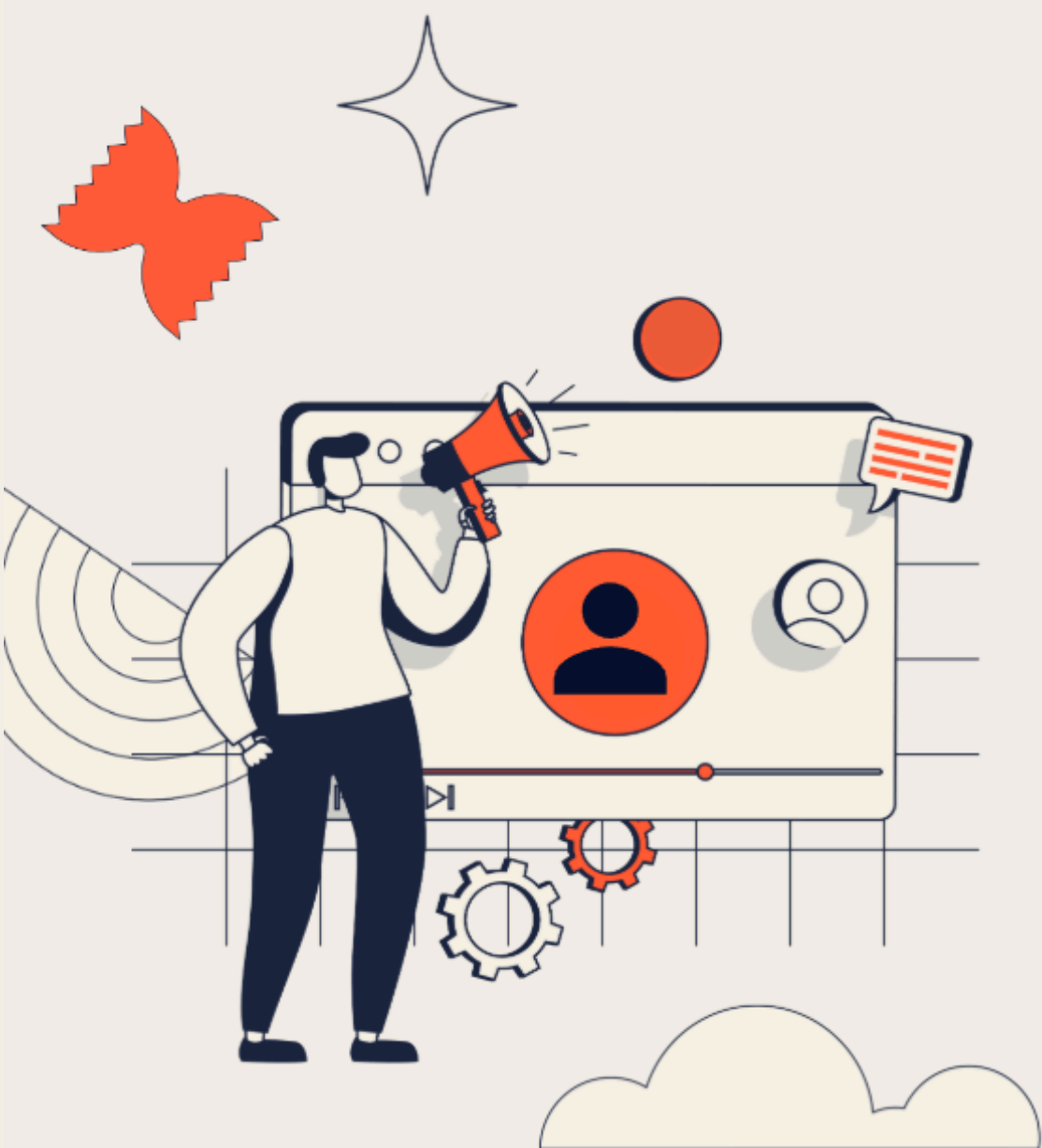


O phishing é uma das principais formas de fraude digital e utiliza mensagens falsas para induzir pessoas a fornecer informações confidenciais, clicar em links maliciosos ou instalar softwares prejudiciais.

- Nunca compartilhe senhas, códigos de autenticação ou outras informações confidenciais por e-mail, telefone ou mensagens;
- Desconfie de mensagens que criem senso de urgência, ameaça ou pressão para uma ação imediata;
- Verifique cuidadosamente o endereço de e-mail do remetente antes de responder ou clicar em links;
- Passe o cursor sobre os links para conferir o endereço real antes de acessá-los;
- Evite abrir anexos de remetentes desconhecidos ou de mensagens inesperadas;
- Utilize apenas canais oficiais para confirmar solicitações de informações ou procedimentos;
- Limite a exposição de informações pessoais e profissionais em redes sociais e ambientes públicos;
- Em caso de dúvida, entre em contato com o suposto remetente por outro meio de comunicação confiável.



Outros golpes comuns no teletrabalho



Smishing e Golpes de WhatsApp: Desconfie de mensagens de texto (SMS) ou no WhatsApp vindas de números desconhecidos se passando pela chefia, colegas de trabalho ou pela STI (Secretaria de TI). Geralmente, usam uma foto copiada da internet e dizem que "mudaram de número" para pedir códigos de ativação ou transferências financeiras.

Vishing (Falso Suporte Técnico): É o golpe por ligação telefônica. Alguém liga dizendo ser do suporte técnico da UFCG, alegando que há um problema urgente no seu computador de trabalho e pede para você instalar um programa de acesso remoto (como AnyDesk ou TeamViewer).



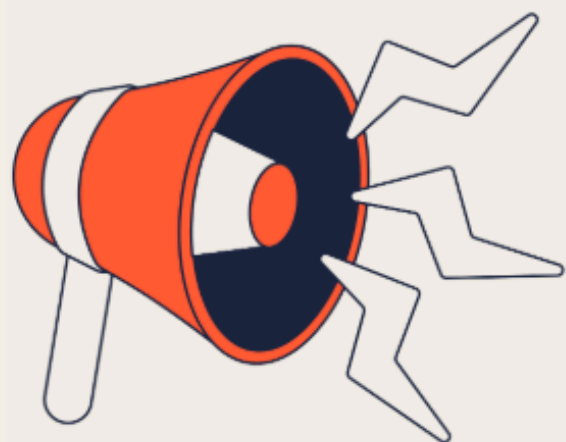
Lei Geral de Proteção de Dados (LGPD) no teletrabalho



O que são Dados Pessoais na UFCG?

Não são apenas o CPF ou o RG. No ecossistema universitário, dados pessoais e sensíveis incluem:

- Históricos acadêmicos e notas de estudantes.
- Folhas de frequência e dados funcionais de servidores.
- Laudos médicos, atestados e relatórios de assistência estudantil (Dados Sensíveis).
- Processos administrativos contendo dados de terceiros dentro do SEI!.



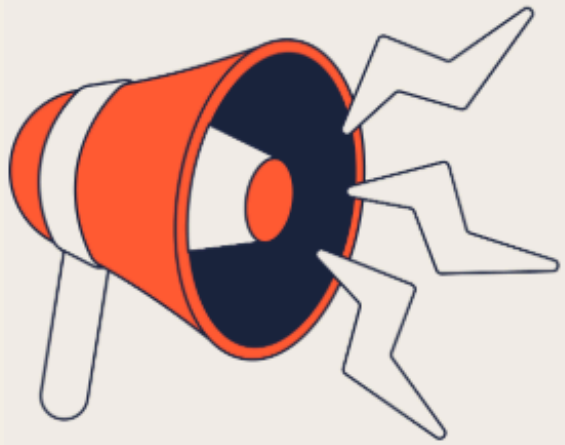
Boas Práticas para o Tratamento de Dados no PGD:

- Acesse e manipule apenas os dados estritamente necessários para realizar a sua tarefa do momento. Se você não precisa ver uma informação para concluir o trabalho, não a acesse.
- Evite trabalhar de costas para janelas abertas ou em locais da casa onde visitas ou prestadores de serviço possam visualizar a sua tela.
- Evite tirar prints de telas de sistemas contendo dados de alunos ou servidores para enviar via aplicativos de mensagem. Se precisar de suporte, oculte os dados pessoais antes de enviar a imagem.
- Toda comunicação que envolva dados pessoais deve ser feita pelo e-mail institucional ou sistemas oficiais (como o Sistema Eletrônico de Informações - SEI!). Não use seu e-mail pessoal para tratar de assuntos da UFCG.



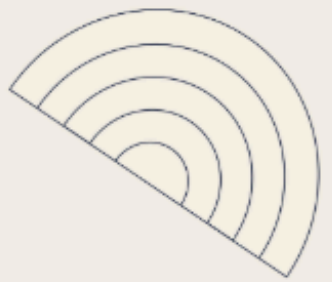


Uso seguro de IA e Arquivos Institucionais



Inteligência Artificial: Produtividade com Responsabilidade

- Ferramentas públicas e gratuitas de IA (como versões abertas do ChatGPT, Claude, etc.) utilizam tudo o que você digita nelas para treinar seus próprios modelos. Inserir um documento interno da UFCG, uma ata de reunião ou um relatório financeiro em uma IA pública equivale a publicar esse documento na internet. **É um vazamento de dados.**
- As IAs criam textos convincentes, mas podem inventar leis, normas, portarias ou dados estatísticos que não existem. Sempre revise criticamente 100% do conteúdo gerado por IA. A responsabilidade legal e administrativa pelo documento final é sempre do servidor, nunca da ferramenta.



Guarda e Compartilhamento de Arquivos Institucionais

- Utilize exclusivamente as soluções de nuvem autorizadas e fornecidas pela UFCG (como o Google Drive/Workspace institucional associado ao seu e-mail @tecnico.ufcg.edu.br, @setor.ufcg.edu.br, ou sistemas próprios da STI).
- Não utilize contas pessoais do Dropbox, OneDrive, Google Drive ou HDs externos particulares para armazenar documentos da Universidade. Se o seu dispositivo pessoal falhar, a instituição perde o rastro daquela informação.
- Ao compartilhar links de pastas ou documentos na nuvem institucional, certifique-se de configurar as permissões corretamente. Evite deixar o link como "Qualquer pessoa com o link pode acessar". Restrinja o acesso apenas aos e-mails dos colegas envolvidos na demanda.
- Mantenha seus arquivos organizados. Documentos temporários ou rascunhos antigos devem ser descartados com segurança para evitar o acúmulo desnecessário de dados obsoletos.



A Segurança Constrói o Futuro do PGD



A flexibilidade e a autonomia trazidas pelo PGD são conquistas valiosas para todos nós e para a UFCG. No entanto, a continuidade e o sucesso desse modelo dependem diretamente da nossa capacidade de manter um ambiente digital seguro, ético e confiável, mesmo fora das instalações físicas da Universidade.

Proteger as informações institucionais e a privacidade da nossa comunidade não é uma tarefa exclusiva da equipe de TI, é um compromisso diário de cada servidor. Cada senha forte que você cria, cada e-mail suspeito que você desconfia e cada tela que você bloqueia funcionam como um escudo que protege a nossa instituição. A segurança não é um obstáculo para o seu trabalho; ela é a garantia de que ele pode ser feito com tranquilidade e eficiência.

Contamos com você. No PGD, o principal escudo da UFCG é você!

