

GUIA DO COLABORADOR

BOAS PRÁTICAS DE PROTEÇÃO DE DADOS - LGPD



CRÉDITOS

Diretoria

Antônio Torres Paz
DIRETOR GERAL

Luciano de Aguiar Monteiro
DIRETOR TÉCNICO

Marcela Jéssica dos S. Oliveira
DIRETORA DE GESTÃO ESTRATÉGICA

José Arimatéia Alves dos Santos
DIRETOR ADMINISTRATIVO FINANCEIRO

Autoria

Raimundo Pereira da Cunha Neto
ENCARREGADO DE TRATAMENTO DE DADOS
PESSOAIS

GUIA DO COLABORADOR SOBRE AS BOAS PRÁTICAS DE PROTEÇÃO DE DADOS



O Programa de Conformidade com a Lei Geral de Proteção de Dados Pessoais da Agência de Tecnologia da Informação do Estado do Piauí - ATI-PI é um chamado para a proteção de dados, continuidade dos serviços tecnológicos e busca incorporar as boas práticas de privacidade no seu dia-a-dia de trabalho.

O que é a LGPD?

A Lei no. 13.709/2018, conhecida como a Lei Geral de Proteção de Dados - LGPD.

Regulamenta o tratamento e guarda de dados pessoais, nos meios físicos e digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

Entrou em vigor em 18 de setembro de 2020.





POR QUE VOCÊ É TÃO IMPORTANTE PARA A PROTEÇÃO DE DADOS?

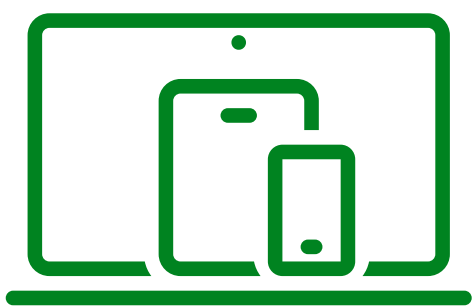
O colaborador da ATI-PI é a base para a proteção de dados e assume um papel importante nessa tarefa, seja por meio do gerenciamento correto das senhas, seja mantendo a segurança de documentos e dados pessoais, ou ainda atentando-se a quem está solicitando as informações.



A maioria dos incidentes de segurança e proteção não são causados por falhas em tecnologia, mas sim por fatores humanos, ou seja, você é a chave para manter a nossa informação protegida.

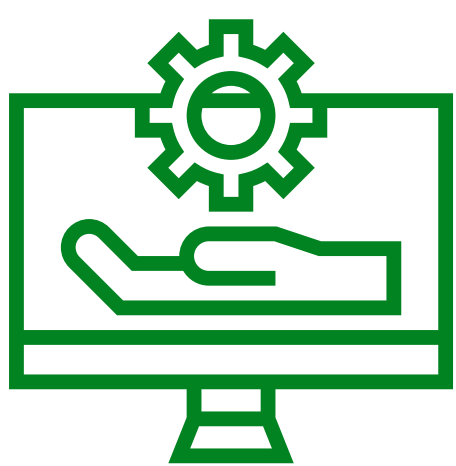


BOAS PRÁTICAS DE PROTEÇÃO DE DADOS



Mantenha seguro os *notebooks*, celulares, *pen-drives* e outras fontes de informações confidenciais em áreas protegidas.

Use criptografia para proteger os dados armazenados nos dispositivos e mídias.



Só utilize *softwares* nos dispositivos da ATI-PI que foram homologados, que venham de fontes oficiais ou que tenham sido devidamente licenciados.

Use conexões seguras, sempre que possível.



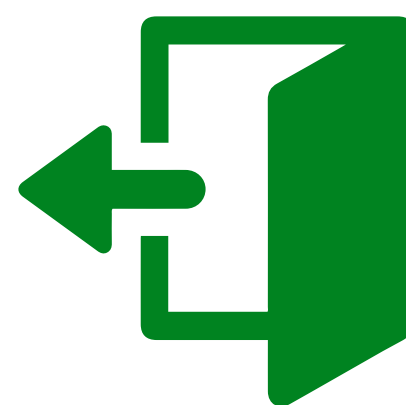


BOAS PRÁTICAS DE PROTEÇÃO DE DADOS



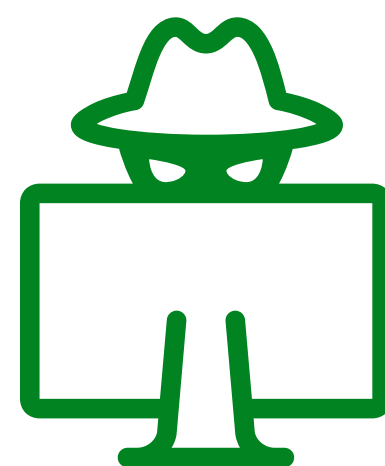
Crie senhas fortes e não repita senhas.

Tenha certeza de sair de suas contas (logout) ao usar equipamentos compartilhados.



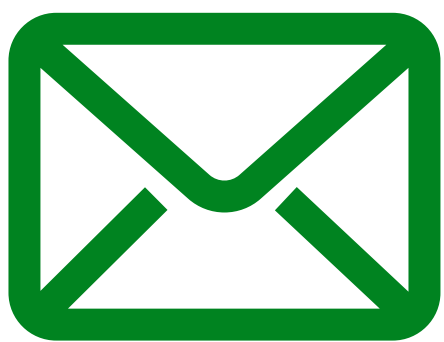
Habilite, quando disponíveis, notificações de login, para ser mais fácil perceber se outras pessoas estiverem usando suas contas ou autenticação de dois fatores.

Verifique o destinatário da mensagem ou link e, em caso de dúvidas, entre em contato direto com o remetente.



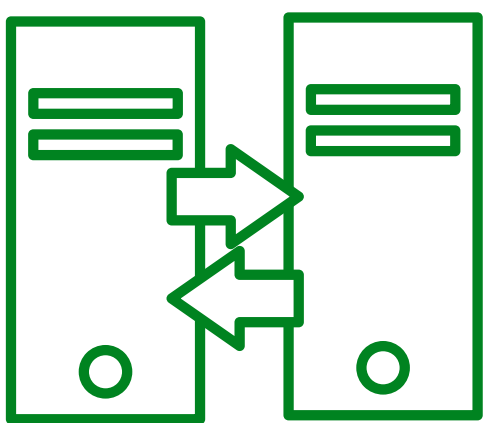


BOAS PRÁTICAS DE PROTEÇÃO DE DADOS



Use sempre o e-mail institucional para comunicações oficiais. Evitar o uso do seu usuário institucional em aplicações ou sites fora da instituição.

Não passe informações confidenciais sem confirmar a identidade do receptor e certificar-se de que ele está autorizado a recebê-las.



Faça backup regularmente. Teste periodicamente e mantenha pelo menos um backup off-line.

Evite colocar na nuvem arquivos contendo dados confidenciais ou que considere privados.



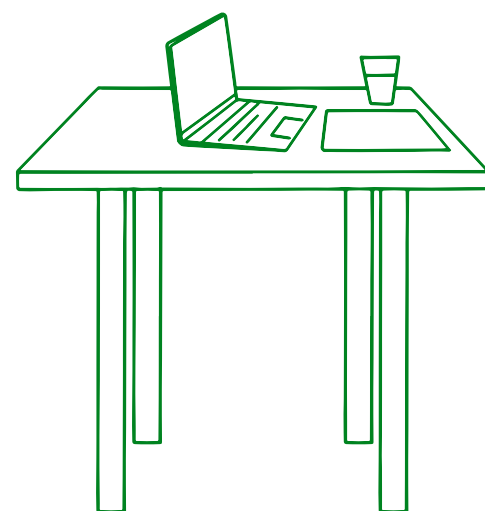


BOAS PRÁTICAS DE PROTEÇÃO DE DADOS



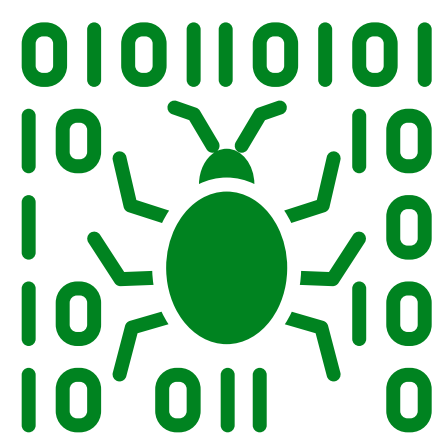
Não jogue papéis com informações confidenciais no lixo comum: destrua-os de maneira apropriada.

Ao sair, deixe a mesa limpa.



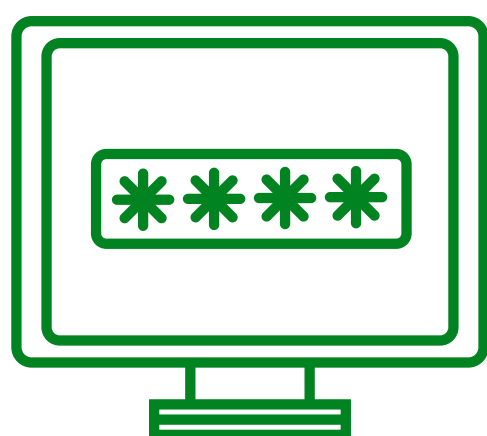
Não responda a mensagens não solicitadas (SPAM), não repasse correntes e não forneça dados pessoais de clientes sem autorização.

Sites externos, downloads e sistemas de mensagens como WhatsApp, podem trazer vírus, arquivos e programas perigosos ao nosso sistema, como roubo de dados.





BOAS PRÁTICAS DE PROTEÇÃO DE DADOS



Não revele a sua senha nem utilize as senhas dos outros. Zele por seu usuário e senha, pois ela é chave de entrada para o SEI e outros sistemas.

Você é responsável por tudo que é feito pelo seu “usuário”. Não anote suas senhas, use a memória para guardá-las.



Atualize o sistema e os aplicativos

Utilize mecanismos de segurança como antivírus, firewall e biometria.





BOAS PRÁTICAS DE PROTEÇÃO DE DADOS



Quando um colaborador for transferido, informe ao setor de TI, para providenciar a mudança de senhas e direitos de acesso. No caso de desligamento, o bloqueio imediato deve ser feito.

Ao se ausentar bloqueie sua estação de trabalho.



Se você perceber alguma falha na segurança, informe imediatamente ao seu gestor ou utilize o canal: dpo@ati.pi.gov.br.



CONTATO DO ENCARREGADO DE DADOS DA ATI



RAIMUNDO PEREIRA DA CUNHA NETO



Data Protection Officer



Av. Pedro Freitas, 1900 – Centro
Administrativo – Bairro São Pedro



Segunda à Sexta das 10:30 as 12:00



dpo@ati.pi.gov.br



(86)9.9443-4720

Maiores informações consulte nosso site
<https://portal.pi.gov.br/ati/>