



UNIVERSIDADE DE SÃO PAULO
REITORIA
GABINETE DO REITOR

São Paulo, 25 de setembro de 2026.

GR/CIRC/349

Prezado(a) Dirigente

A Universidade de São Paulo fundamenta sua atuação na excelência acadêmica e na confiança da sociedade. No mundo contemporâneo, essa confiança é construída e mantida, em grande parte, por meio da nossa presença no ambiente digital. As páginas *web* das Unidades, Departamentos e Laboratórios são frequentemente o primeiro ponto de contato para alunos, pesquisadores, parceiros internacionais e para a imprensa.

Neste sentido, a Superintendência de Tecnologia da Informação (STI) vem monitorando um crescimento preocupante no número de ataques cibernéticos direcionados aos *sites* mantidos pelas Unidades da USP. O principal foco dessas investidas é uma prática conhecida como **defacement** (desfiguração de página). Trata-se de uma invasão na qual criminosos alteram o conteúdo visual e as informações dos nossos *sites* sem autorização, substituindo informações acadêmicas legítimas por mensagens de protesto, conteúdos ilícitos ou redirecionamentos para fraudes eletrônicas.

A maioria dos *sites* institucionais da USP é construída sobre plataformas chamadas Sistemas de Gerenciamento de Conteúdo (CMS), como o WordPress, o Drupal e o Joomla!. O CMS é o *software* que possibilita à equipe técnica da sua Unidade criar, editar e gerenciar as publicações do *site* de forma prática, sem a necessidade de escrever códigos complexos de programação.

No modelo de serviços de TI da Universidade, a STI é responsável por prover a máquina, manter o servidor funcionando e proteger a rede geral. No entanto, a instalação, a configuração e a **atualização contínua do software CMS** são de inteira responsabilidade das equipes técnicas (usuários do sistema) alocadas em cada Unidade.



Os cibercriminosos exploram, quase que exclusivamente, *sites* que utilizam versões antigas e desatualizadas desses *softwares* CMS e de seus complementos (*plugins*). Quando um *site* deixa de receber as devidas atualizações de segurança, ele se torna um alvo fácil, permitindo que invasores tomem o controle da página de maneira automatizada.

O impacto de ter o *site* da sua Unidade invadido vai muito além do simples transtorno tecnológico. As consequências incluem:

1. **Dano Reputacional e Perda de Credibilidade:** um *site* desfigurado com mensagens impróprias transmite uma imagem imediata de negligência e fragilidade. Isso pode abalar severamente o prestígio acadêmico da instituição, gerando desconfiança em agências de fomento, parceiros internacionais e no público em geral.
2. **Bloqueio em Buscadores:** *sites* invadidos são rapidamente identificados por buscadores, como Google, que passa a exibir telas vermelhas de alerta (“Site Enganoso”), bloqueando o acesso e removendo a página dos resultados de pesquisa. A reversão dessa penalidade é lenta.
3. **Risco de Violação de Dados Pessoais:** a brecha tecnológica que permite a alteração do *site* é frequentemente a mesma que permite aos invasores roubar dados coletados pela página (sistemas) e armazenados localmente na Unidade, sujeitando a Universidade a pesadas sanções legais previstas na Lei Geral de Proteção de Dados (LGPD).
4. **Vazamento de Credenciais de Acesso:** as credenciais administrativas expostas durante a invasão do CMS podem conter senhas idênticas às utilizadas na Senha Única USP. Como a reutilização de senhas é uma prática recorrente, invasores podem usá-las para comprometer contas institucionais e obter acesso não autorizado a *e-mails*, sistemas internos e bases de dados sensíveis da Universidade.

Diante da gravidade e do risco institucional envolvido, solicitamos a intervenção urgente de V. Sa. junto à equipe técnica e de Tecnologia da Informação de sua Unidade. É imperativo que seja realizada uma força-tarefa imediata para:

- verificar e aplicar, com urgência, todas as atualizações de segurança pendentes nos sistemas CMS (e.g. WordPress, Drupal e Joomla!) sob responsabilidade da Unidade;

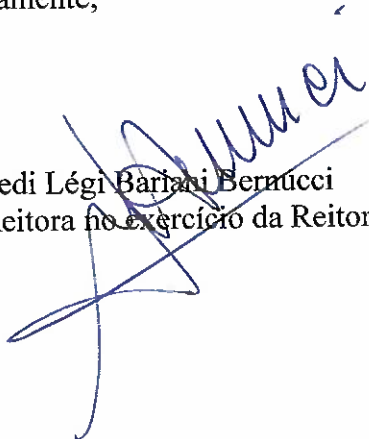


- desativar e remover completamente complementos (*plugins* ou temas) que não estejam mais em uso;
- estabelecer rotinas semanais e permanentes de verificação de atualizações;
- atualizar as senhas utilizadas para acesso aos bancos de dados.

A segurança da informação é um esforço coletivo e ininterrupto. A STI e a equipe de Resposta a Incidentes (CSIRT USP) permanecem à inteira disposição, por meio do *e-mail* security@usp.br, para orientar e prestar o apoio consultivo necessário às equipes locais.

Contamos com a sua imprescindível colaboração para que possamos proteger o patrimônio digital e a credibilidade da Universidade de São Paulo.

Atenciosamente,


Liedi Légi Bariani Bernucci
Vice-Reitora no exercício da Reitoria