COMUNICA
Informativo eletrônico destinado aos servidores
Universidade Federal Fluminense

Redobre a sua atenção com a segurança digital no trabalho remoto.

Uma das grandes diferenças do trabalho remoto para o presencial diz respeito aos mecanismos de proteção e segurança digital. Enquanto realizávamos as nossas atividades nos computadores da UFF e com acesso à rede interna, não existiam tantos questionamentos e preocupações com a atualização das máquinas, instalação de antivírus, criação de senhas etc.

Algumas vulnerabilidades impostas por esse modelo de trabalho, como os ataques cibernéticos ainda mais frequentes, nos levam a buscar alternativas para a realização das atividades de modo seguro, que evitem inclusive o vazamento de dados e o compartilhamento em rede de informações sigilosas, não somente da Universidade como também as de cunho privado. Isso é válido sobretudo para aqueles que executam as tarefas do dia a dia direto de dispositivos pessoais, como seus próprios computadores, notebooks e smartphones.

É por essa razão que, em parceria com a Superintendência de Tecnologia da Informação (STI), levantamos alguns tópicos sobre segurança digital para serem levados a sério por você, servidor (a)! Acompanhe as dicas e coloque-as em prática.

1 - Escolha adequada do antivírus

O primeiro passo para evitar surpresas no ambiente digital de trabalho é a escolha de um bom antivírus. Atualmente, existem muitos softwares gratuitos e com excelente reputação. Mesmo se o seu computador for de última geração, não dispense a instalação do antivírus na sua máquina ou smartphone.

E mais: mantenha o antivírus atualizado; configure-o para verificar automaticamente toda e qualquer extensão de arquivo, arquivos anexados

aos e-mails, obtidos pela Internet, os discos rígidos e as unidades removíveis; evite executar simultaneamente diferentes antivírus (eles podem entrar em conflito, afetar o desempenho do equipamento e interferir na capacidade de detecção um do outro). A equipe da STI sugere alguns gratuitos que podem ser visualizados **neste link**.

2 - Atualize o PC e softwares

Nunca descarte a sugestão de atualização de segurança do seu desktop, notebook, smartphone e softwares. As atualizações foram feitas justamente para corrigir pequenos erros e minimizar os riscos de invasão por terceiros e outros. Outra recomendação é não instalar programas suspeitos. Sempre que possível, opte pelos originais.

3 - Evite o uso de fontes não confiáveis para conversão de documentos

Muitas vezes nos vemos obrigados a converter arquivos oficiais da Universidade com extensão DOC para PDF e vice-versa, além de outros. Não é recomendável que documentos sigilosos ou confidenciais sejam distribuídos na internet (em sites que têm esse objetivo) ou submetidos a ferramentas de terceiros para algum tipo de manipulação. Dependendo da conversão, plataformas como Microsoft Office e LibreOffice já realizam este procedimento. Saiba mais nestas orientações externas: **https://bit.ly/3x6cdaS** e **https://convertio.co/pt/**

4 - Crie senhas fortes para acesso aos dispositivos e rede wi-fi

Esqueça desde já a criação de senhas com datas de nascimento, nome do filho ou sobrenome. É o segredo da senha que garante a sua identidade no acesso aos diferentes dispositivos (computadores, roteador, rede wi-fi etc) e vai minimizar os riscos envolvidos no uso da internet, como quando acessamos o e-mail pessoal ou corporativo.

Por isso, use senhas longas, compostas de diferentes tipos de caracteres; não as deixe anotadas em locais onde outras pessoas possam vê-las); evite digitá-las em computadores e dispositivos móveis de terceiros; evite salvar as suas senhas no navegador Web ou usar opções como “Lembre-se de mim” e "Continuar conectado”; evite usar a mesma senha para todos os serviços que você acessa.

5- Proteja-se de phishing e códigos maliciosos

Phishings nada mais são do que mensagens atrativas usadas por hackers para o roubo dos dados pessoais, bancários e outros do usuário. Por isso, desconfie de mensagens recebidas, mesmo que enviadas por conhecidos; evite seguir links recebidos em mensagens eletrônicas; não utilize um site de busca para acessar serviços que requeiram senhas, como seu E-mail e suas redes sociais; seja cuidadoso ao acessar links reduzidos.

6 - Armazene na nuvem documentos e outros arquivos.

O armazenamento em nuvem é ideal para salvar, criar, editar e compartilhar documentos, planilhas e outros conteúdos importantes com segurança e praticidade entre as equipes. Aqui na UFF, todos os servidores com email institucional (@iduff) possuem acesso ao Google Drive. Ao armazenar na nuvem, você evita inclusive o uso de pen drives e HDs externos, dispositivos que podem estar infectados. Saiba mais sobre o armazenamento digital na Universidade: **https://bit.ly/3js0wXR**

7 - VPN (acesso seguro a rede de internet doméstica)

Utilizar uma VPN (Rede Privada Virtual) em seu computador ou notebook possibilita que você acesse a rede local da Universidade à distância e de forma segura. Quando você se conecta a uma VPN, sua comunicação com a internet é criptografada e protegida de interceptação. Ela proporciona mais segurança à navegação, evitando que cibercriminosos acessem seus dados.

Alguns sistemas da Universidade só podem ser acessados fora da UFF por meio de uma VPN. Saiba mais nos **manuais disponíveis pela STI**.

Cursos e oportunidades

Excelente oportunidade para quem desenvolve projetos de extensão na Universidade! O Programa de Fomento à Ações de Extensão (FOEXT) está com edital aberto para submissão de propostas. Nessa segunda edição, o recurso destinado é de R$ 250 mil reais e vai contemplar até 50 propostas.

O objetivo do FOEXT é ampliar e apoiar ações de extensão na UFF, fomentando a aquisição de material de consumo para e pequenos serviços realizados por Pessoas Jurídicas (PJ). Fique atento no prazo de registro da Ação de Extensão no sistema: 21 de julho.

Saiba mais **aqui**.

De olho na UFF

Começou mais um período de Avaliação de Desempenho dos servidores da UFF. Como ocorre desde o início da pandemia, todos os trâmites são digitais, já que a Progepe encaminha os formulários avaliativos e os Planos de Trabalho às Direções das Unidades, que deverão proceder à distribuição interna, entre as chefias dos setores e os respectivos servidores.

Atenção para o prazo de retorno dos formulário:

- 19/07 a 23/07/21 - Devolução das avaliações com vigência em julho/2021;
- 23/08 a 26/08/21 - Devolução das avaliações com vigência em agosto/2021;
- 20/09 a 24/09/21 - Devolução das avaliações com vigência em setembro/2021.

Leia o informe completo no **site da UFF**.

O Programa “Tempo de Cuidar: compartilhando vivências”, da Equipe de Psicologia da Divisão de Assistência à Saúde (CASQ/Progepe), está lançando mais um grupo psicoterapêutico online! Saiba mais:

Grupo Terapêutico 2 - Focado em servidores com quadros crônicos de saúde física e mental
- Início: 22/07/2021
- Encontros: Quintas-feiras, 14h, via Google Meet. Máximo de 8 participantes.
- Inscreva-se até 20/07 pelo formulário: **bit.ly/G2TempoDeCuidar**
- E-mail para dúvidas: sps.das.casq@id.uff.br

Informes

Divisão de Transporte da UFF ganha canal de comunicação via Whatsapp

Operações e Manutenção na UFF - Relatório de Gestão do mês de maio

E-Book Grátis - Engajamento social: contribuições para o ensino de graduação

Resultados da Gestão de Riscos

Parada programada: Sistema de Chamados - 02 de julho

Veja todos os informes

Agenda de lives

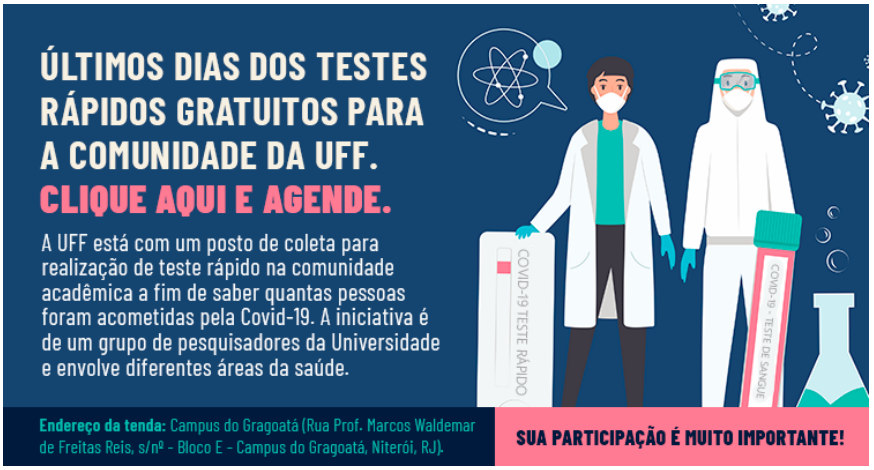
Ep. 03 PODCAST - OSN 60 anos, a nossa orquestra!
Dia 02/07, às 10h, pelo canal do Spotify do Centro de Artes

I Encontro do Fórum Estadual dos GT sobre Equidade de Gênero, Parentalidade e Diversidade das IES RJ
Dia 02/07, às 16h, pelo canal do Youtube do Fórum

IV Conect Virtual
Dia 06/07, às 15h - Inscrições abertas

X Lean Six Sigma Congress - SUBMETA SEU RESUMO!
Submissão de propostas: até 11 de julho

Veja todas as lives



da Universidade Federal Fluminense

Caso não tenha recebido alguma edição, **visualize aqui**