FACEPE
Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA FACEPE

Este termo de uso tem como objetivo padronizar e estabelecer requisitos mínimos de segurança, a fim de proporcionar condições de segurança da informação e proteção aos equipamentos. Os itens descritos neste termo aplicam-se a todos que fazem uso dos serviços disponibilizados pela UTIC.

I. Utilização de recursos tecnológicos

- Todos devem ter consciência de que os computadores, a rede e os demais serviços e equipamentos disponibilizados pela UTIC devem ser usados apenas para desempenhar suas atividades profissionais na FACEPE (e não para fins pessoais);

- Os equipamentos, serviços e sistemas institucionais são de propriedade da Fundação e podem ser recolhidos ou auditados conforme necessário;

- No caso de qualquer problema no funcionamento dos computadores, deve-se solicitar à UTIC a correção do problema. O colaborador não deve tentar resolver o problema por conta própria. Não se deve abrir equipamentos, nem substituir por conta própria;

- No caso de qualquer problema nas impressoras, deve-se comunicar à UTIC para que seja feito o devido reparo, não devendo o colaborador tentar resolver o problema por conta própria;

- No caso de necessidade de deslocar qualquer equipamento tecnológico (computador, teclado, mouse, antena de Wi-Fi, projetor, filtro de linha, etc.), deve-se também solicitar essa mudança à UTIC, ainda que seja apenas mudança para a mesma sala, ou mesmo para substituição de mouse/teclado.

- É de responsabilidade do colaborador o backup dos seus arquivos importantes para o desempenho das funções sob sua responsabilidade. É recomendado o uso de ferramenta de sincronia de documentos em nuvens (Google Drive);

- Antes de ausentar-se da sua mesa de trabalho, o usuário deve bloquear seu computador (Tecla Windows + L), como forma de aumentar a segurança do uso de seu perfil;

- Ao término do expediente deve-se desligar o computador e monitor;

- Instalações ou remoções de softwares deverão ser efetuadas pela UTIC; Não se deve utilizar qualquer tipo de software nem conectar qualquer dispositivo que não esteja relacionado às funções e atividades da FACEPE. Não se deve conectar dispositivos para uso pessoal nas redes da FACEPE;

- É proibido colar adesivos, figuras e similares nos equipamentos computacionais, ressalvada a colagem feita pela UTIC e pelo patrimônio para identificação do equipamento.

II. Utilização do E-mail Corporativo

- O e-mail corporativo deve ser usado apenas para o desempenho das funções do colaborador;
- O uso da lista "todoscolaboradores@facepe.br" deve ser restrito para tratar de assuntos relacionados à FACEPE.

III. Utilização do acesso à Internet

- A rede de acesso à internet deve ser usada apenas como apoio ao desempenho das funções da FACEPE.
- Caso a Fundação julgue necessário, ocorrerão bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede ou aqueles que exponham a rede a riscos de segurança.

Condutas recomendadas:

- Zelar pela integridade dos componentes do computador, deixando-o sempre limpo, longe de comida e líquidos;
- Comunicar à UTIC, por meio de solicitação através do Helpdesk, qualquer problema com os serviços de rede, computadores, internet, e-mails e impressoras da instituição;
- Quando o colaborador perceber oscilações na rede elétrica (ex: luz da sala piscando, equipamentos desligando), os usuários devem salvar os documentos em uso e desligar os equipamentos e o filtro de linha até que sejam informados sobre a normalização da rede elétrica. Caso o equipamento já tenha sido desligado pela queda de energia, deve-se desligar o filtro de linha;
- Manter o sigilo das suas senhas de acesso à rede e aos sistemas.

Disposições finais:

Compete ao Comitê de Privacidade da Facepe (grupo de apoio designado na Portaria n° 13/2021) a gestão da Segurança da Informação:

- Promover a disseminação e conscientização da segurança da informação na Fundação;
- Deliberar sobre os recursos necessários para que ações de segurança da informação sejam executadas;
- Aprovar a atualização da Política de Segurança da Informação (PSI), propondo revisão e novas políticas específicas, bem como procedimentos que assegurem o controle das ações de política de segurança da informação;
- Acompanhar as atividades do plano de incidentes de segurança da informação tecnológica que comprometam dados e/ou a imagem da Facepe;
- Deliberar sobre as estratégias para mitigar as possíveis causas das vulnerabilidades exploradas.