tecnologia a serviço da cidade
procempa

Política de Uso Geral da Rede e Equipamentos

Julho, 2022

Política de Uso Geral da Rede e Equipamentos

1. Os equipamentos, serviço de chat, correio eletrônico com o endereço profissional da PROCEMPA e acesso a rede são fornecidos para atividades e finalidades de trabalho. A PROCEMPA respeita o direito a privacidade, mas se reserva o direito de buscar conteúdos com finalidade profissional nos seus equipamentos e investigar violações às normas, quando julgar necessário, a seu critério.
2. Os acessos feitos com o uso de equipamentos da companhia ou em sua rede corporativa podem ser monitorados e registrados pela PROCEMPA.
3. A PROCEMPA pode bloquear ou não, a qualquer tempo, em seus equipamentos ou em sua rede corporativa o acesso a recursos, sitios e serviços que considerar inadequados, ilegais ou inseguros.
4. O compartilhamento de recursos nas estações de trabalho e equipamentos conectados na rede corporativa deve ser limitado a atividades de interesse da companhia, com liberação somente para leitura ou para conjunto restrito de usuários.
5. Não é permitido instalar, usar ou configurar equipamentos, hardware ou software que deem acesso externo à rede corporativa sem autorização formal e conhecimento da Equipe de Segurança da Informação. Em especial, não é permitida a instalação de ponto de acesso wifi, bluetooth, modem, vpn ou software de acesso remoto sem essa autorização.
6. Usando quaisquer recursos da PROCEMPA, é vedado o envio de mensagens com correntes, conteúdo eleitoral, difamatório, ofensivo, preconceituoso, obsceno, pornográfico ou que dê margem a interpretação de discriminação racial, sexual, religiosa ou política.
7. Não é permitido distribuir usando recursos da PROCEMPA ou em seu nome mensagens comerciais não solicitadas (spam).
8. Notebooks, laptops, tablets e outros equipamentos pessoais ou de terceiros não poodem ser ligados na rede corporativa da PROCEMPA sem autorização expressa. Manter atualizações e proteção adequada antivírus nesses equipamentos é de responsabildade do usuário. Tais equipamentos podem ser conectados à rede wifi e ter acesso a serviços internos via VPN gerenciada pela companhia para essa finalidade, seguindo as normas da Equipe de Segurança da Informção. Em qualquer caso, a companhia não se responsabiliza por danos e acessos indevidos a esses equipamentos ou aos dados neles armazenados.

Proteção de Estações

1. Todas as estações de trabalho, notebooks e laptops da PROCEMPA devem ter instalado, ativo e atualizado o antivírus corporativo indicado pela Equipe de Segurança da Informação.
2. O usuário não deve impedir a operação e atualização do antivírus sem autorização e conhecimento da Equipe de Segurança da Informação.
3. Constatado qualquer problema com o antivírus, o usuário deverá comunicar a Equipe de Segurança da Informação que tomará as providências cabíveis.

Utilização de Software

1. As estações de trabalho e notebooks são disponibilizadas com os programas – sistema operacional e aplicativos – mínimos necessários para o desempenho de sua função básica. A instalação de aplicativos adicionais para fins de trabalho pode ser solicitada para a Equipe de Tecnologia da Informação. Tais aplicativos devem estar adequadamente licenciados, homologados, inventariados e em conformidade com as normas, com aprovação da Equipe de Segurança da Informação.
2. São considerados legítimos os softwares instalados e utilizados para fins de trabalho, conforme suas licenças de uso e que não contrariem as demais normas da companhia e legislação. Em especial, esta norma contempla a possibilidade de uso de software livre para fins legítimos de trabalho e não abusivos.
3. Não é permitida a instalação nos equipamentos da companhia de qualquer software, gratuito ou não, sem a licença compativel para uso comercial pela PROCEMPA. Dessa forma, não são permitidos uso ou instalação de softwares com licença apenas para uso pessoal ou em nome de individuo, mesmo que seja em nome do próprio usuário. Violações a essa norma podem caracterizar pirataria, ficando usuário e instalador sujeitos a sanções administrativas, legais e penais.
4. Ocasionalmente serão realizadas verificações no inventário dos equipamentos, com relação a hardware e software permitindo identificar desvios das normas.

Credenciais e Identificações

1. Identificações, credenciais ou senhas devem ser individuais e mantidas em sigilo, não devem ser transferidas ou compartilhadas.
2. Cada funcionário deve trocar periodicamente suas senhas e é sua responsabilidade escolher senhas robustas, complexas e longas, inéditas, difíceis de serem adivinhadas.
3. As senhas devem ser únicas, não podem ser usadas senhas idênticas ou semelhantes para identificação em sistemas, sítios ou serviços não gerenciados pela PROCEMPA, sejam de natureza pessoal ou não.
4. Contas institucionais da PROCEMPA em quaisquer sistemas, redes sociais, sítios ou serviços devem necessariamente ter ativos Múltiplos Fatores de Autenticação sempre que a opção estiver disponível.
5. Senhas, certificados, chaves criptograficas e suas cópias podem ser armazenadas criptografadas em aplicativos para essa finalidade indicados pela Equipe de Segurança da Informação, mas não é permitido armazenar cópias sem criptografia em arquivos digitais ou físicos. Mesmo criptografadas, as midias físicas que as contém devem ser mantidas em local protegido contra roubos e furtos.