

Boa tarde,

Favor descrever os itens conforme solicitado no CHECKLIST:

PC 07 - 5.2 CONTROLE DE ACESSO A SISTEMAS E SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

5.3 SELEÇÃO E USO DE SENHAS

A liberação do acesso aos recursos de TI do empregado deve ser solicitada via Sistema de Chamados da Central de Serviços da GETIN, imediatamente após sua admissão ou remanejamento, pela Gerência de Recursos Humanos - GEREH.

No caso de liberações para acesso de terceirizados, a solicitação deverá ser realizada pelo gerente da área interessada

Senhas são de uso pessoal e intransferível, sendo sua manutenção e confidencialidade responsabilidade de seu proprietário

Senhas não devem ser registradas em papel, ou em qualquer meio sem controle ou caracterizado como de acesso público

As senhas devem conter o padrão mínimo de 6 (seis) caracteres, atendendo ao menos 3 critérios, sendo eles: letra maiúscula, letra minúscula, números e símbolos

Senhas temporárias ou iniciais devem ser alteradas pelo usuário no primeiro acesso, conforme regras estabelecidas nesta norma

Senhas de acesso aos recursos de informática devem ser alteradas periodicamente, evitando a reutilização de senhas antigas. Caso esse procedimento não seja realizado pelo usuário, o sistema automaticamente solicitará a cada 3 meses, uma nova senha ao usuário

O acesso (conta) aos recursos de TI será bloqueado após 5 (cinco) tentativas com erro

Senhas devem ser alteradas pelos usuários, sempre que existir qualquer indicação de possível comprometimento do sistema, ou das próprias senhas. Na criação e alteração da senha de acesso à rede e aos sistemas de informação deve-se evitar a utilização de:

- a) Nome próprio ou sobrenome do usuário;
- b) Nome de parentes ou time de preferência;
- c) Datas comemorativas;
- d) Sequência de números e letras;
- e) Conjunto de caracteres totalmente iguais;
- f) Conjunto de caracteres iguais à conta;

g) Informações que possam ser obtidas do próprio usuário, tais como: telefone, número da identidade, número do CPF, placa de carro, etc.

PC 07 - 5.4 USO DE ATIVOS DE INFORMAÇÃO

5.6 INSTALAÇÃO E UTILIZAÇÃO DE SOFTWARES

5.7 PROTEÇÃO DAS INFORMAÇÕES

5.12 USO DOS SISTEMAS DE INFORMAÇÃO

A conexão de equipamentos de terceiros (empregados e prestadores de serviço) à rede corporativa da EMAP deve ser solicitada através do Sistema de Chamados da Central de Serviços da GETIN pela Diretoria ou Gerência da área interessada, cabendo a Gerência de Tecnologia da Informação, autorizar ou não esta conexão.

Somente a Gerência de Tecnologia da Informação é autorizada a executar a conexão de equipamentos de terceiros à rede corporativa da EMAP, não sendo permitido a nenhum outro setor, executar este procedimento.

Os equipamentos de informática funcionarão somente com softwares regularmente adquiridos e licenciados junto a seus fornecedores ou representantes, ou ainda, aquele fruto de desenvolvimento personalizado para EMAP.

São expressamente proibidas seguintes atividades:

- a) Cópia de softwares adquiridos ou desenvolvidos pela EMAP, seja qual for a finalidade;
- b) Instalação de softwares nos ativos de informação da EMAP;
- c) Modificação ou distribuição de dados ou programas sem autorização.

Em caso de violação às medidas de segurança das informações, a GETIN deve efetuar o bloqueio do acesso do usuário à rede, e comunicar o fato ocorrido, imediatamente ao responsável pela área onde ocorreu a violação, para que sejam aplicadas advertências ou sanções cabíveis.

Para prestadores de serviço que necessitam de acesso aos sistemas de informação, é necessário que o gestor da área responsável envie uma solicitação através do Sistema de Chamados da Central de Serviços da GETIN, informando os dados do usuário.

PC 07 - 5.5 COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

Quaisquer incidentes de segurança, que ocorram nas localidades remotas de trabalho, tais como roubos, invasões, ataques por vírus, deverão ser imediatamente comunicadas à Gerência de Tecnologia da Informação, para que as medidas apropriadas sejam tomadas

O trabalho remoto à infraestrutura da EMAP somente será autorizado quando for de estrito interesse da empresa, devendo ser precedida de solicitação do gestor do setor do empregado e análise quanto a sua necessidade, viabilidade

e autorização formal da GETIN

Todo acesso remoto autorizado deverá possuir prazo de expiração que poderá ser renovado mediante solicitação do gestor do setor do empregado e análise quanto a sua necessidade, viabilidade e autorização formal da GETIN.