MINISTÉRIO DA EDUCAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAIANO

CAMPUS URUÇUCA

POLÍTICA DE GESTÃO DOS RECURSOS E SERVIÇOS DE TI

NÚCLEO DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

Versão 4

URUÇUCA
ABRIL/2024

Conteúdo

OBJETIVO

O objetivo deste documento é nortear a gestão dos **recursos** e **serviços** de TI com enfoque nos princípios de segurança da informação.

DA POLÍTICA

1. O **NGTI** é responsável pela redação e revisão deste documento.

2. Esta política deverá ser atualizada toda vez que houver necessidade de correções ou adequações às possíveis mudanças no quadro de **recursos** e **serviços** de TI do campus.

3. Este é um documento complementar que trata aspectos específicos da gestão de **recursos** e **serviços** de TI do campus, mas que observa todos os demais dispositivos legais que tratam da mesma matéria no âmbito da instituição.

DAS SANÇÕES

1. As violações aos termos desta política devem ser analisadas como **infrações administrativas**, cabendo às respectivas chefias ou imediatos as avaliações de sanções de acordo ao que concerne as leis correspondentes e aos regimentos da instituição.

DISPOSIÇÕES GERAIS

1. A gestão dos recursos e serviços de TI deve seguir os padrões estabelecidos na **Documentação de Procedimentos Técnicos** (**DPT**).

2. Todas as ações referentes a gestão dos recursos e serviços de TI devem ser registradas no **Sistema de Gestão de Tecnologia da Informação** nos seguintes moldes:

   a) Inventário completo dos recursos e serviços de TI;
   b) Dados dos contratos dos serviços externos/indiretos;
   c) Processos de **mudanças** nos recursos ou serviços de TI;
   d) Processos de resolução de **problemas** nos recursos e serviços de TI;
   e) **Projetos** de implantação e/ou configuração de recursos e serviços de TI;

3. Fica estabelecido como o **Sistema de Gestão de Tecnologia da Informação** o software livre **GLPI**.

4. Os membros do NGTI devem manter e prezar pela confidencialidade, integridade e disponibilidade de todos os dados e informações aos quais tiverem acesso no desenvolvimento de suas atividades.

GESTÃO DOS COMPUTADORES INSTITUCIONAIS

1. É proibida a violação física dos computadores institucionais durante o período de vigência dos contratos de garantia e suporte, exceto quando permitido pela contratada.

2. O programa CMOS Setup dos computadores institucionais devem ser protegidos por senha conforme documento específico da **DPT**.

3. A gestão dos usuários locais nos sistemas operacionais (SOs) dos computadores institucionais é restrita ao NGTI e deve ser realizada conforme documento específico da **DPT**.

4. Todos os computadores institucionais devem conter os programas da **Lista de Softwares Homologados**, que é criada de forma a atender as necessidades dos usuários em suas atividades relacionadas ao campus.

5. Os softwares instalados nos computadores institucionais devem ser obtidos em mídias originais, sites dos desenvolvedores ou repositórios oficiais.

6. Os SOs e os softwares dos computadores institucionais devem ser mantidos sempre atualizados.

7. Anualmente ou semestralmente, conforme a necessidade, preferencialmente durante os períodos de recessos acadêmicos, deverá ser executada a **Rotina de Clonagem e Padronização** em todos os computadores institucionais, cujos procedimentos são indicados em documento específico da **DPT**.

GESTÃO DA REDE LOCAL

1. Somente os dispositivos institucionais gerenciados e homologados pelo NGTI poderão ser conectados aos seguimentos da rede local que dão acesso a todos **serviços de TI.**

2. Apenas o **Serviço de Acesso à Internet** poderá também ser disponibilizado a dispositivos pessoais ou institucionais não gerenciados, mas através de redes Wi-Fi específicas.

3. As redes Wi-Fi que dão acesso aos seguimentos da rede local para os usuários devem ser protegidas com o padrão de segurança **IEEE 802.1X**, exceto a rede aberta para os usuários não vinculados à instituição ou à rede CAFe.

4. É proibida a execução de softwares de *hacking* ou *pentest* na rede local do campus, exceto quando executados pelo NGTI com a finalidade de identificar e suprimir vulnerabilidades. Neste caso o NGTI deve informar aos usuários da rede anteriormente a realização dos procedimentos.

5. Os firewalls da rede devem ser configurados com política restritiva, priorizando-se sempre a negativa dos acessos e autorizando apenas o que for estritamente necessário.

6. Os servidores cujas aplicações ou serviços sejam publicados na internet constituem a **DMZ** e devem receber IP público da **RNP** conforme disponibilidade.

7. Os servidores da **DMZ** devem ter seus próprios firewalls configurados seguindo a mesma política restritiva dos firewalls de borda.

8. O gerenciamento e a segurança dos servidores da **DMZ** que não são administrados pelo NGTI é de responsabilidade exclusiva do seu respectivo proprietário.

GESTÃO DOS SERVIDORES E SERVIÇOS DA REDE

1. Os SOs e as aplicações dos servidores da rede devem ser mantidos sempre atualizados.

2. É proibida a instalação de outros softwares nos servidores além do que é estabelecido pela **lista de softwares homologados** e suas respectivas documentações da **DPT**.

3. Os softwares instalados nos servidores devem ser obtidos em mídias originais, sites dos desenvolvedores ou repositórios oficiais.

4. A rotina de atualizações dos servidores deve respeitar o período estabelecido na **planilha de eventos da rede**, podendo as atualizações de segurança serem aplicadas de forma imediata.

5. Todas as atualizações dos servidores devem ser precedidas de um snapshot (em VMs) ou criação de imagem de disco (em servidores físicos), podendo-se descartar os arquivos de backup uma semana após a respectiva atualização, caso nenhuma inconsistência seja apresentada.

6. Deve se evitar o uso das contas de usuários locais no acesso às consoles dos servidores e aplicações da rede, sendo sempre recomendado o uso das credenciais individuais.

7. Os logons nos servidores devem ser realizados por motivos de intervenções técnicas, e devem ser evitados para qualquer outra finalidade.

8. As sessões de logon nos servidores devem sempre ser encerradas após os acessos às suas respectivas consoles.

POLÍTICA DAS AUTENTICAÇÕES, AUTORIZAÇÕES E ACESSOS (AAA'S)

1. Fica instituída a aplicação **Active Directory (AD)** como solução de autenticação central da rede, de modo que todos os dispositivos, sistemas e serviços, sempre que possível, devem ser configurados para autenticar e autorizar os acessos através dessa aplicação.

2. Todas as AAA's nos recursos e serviços de TI devem ser registradas e encaminhadas aos servidores de log da rede.

3. É proibido o compartilhamento ou uso indevido dos registros das AAA's, e esses dados devem ser utilizados apenas para apuração de denúncias ou suspeitas de violação às políticas de uso e gestão dos recursos e serviços de TI.

4. As senhas dos usuários cadastrados no AD devem atender aos requisitos de complexidade sugerido pela aplicação.

5. As senhas dos usuários locais nos dispositivos da rede devem seguir os mesmos critérios de complexidade referido no item anterior.

6. As senhas dos usuários locais nos dispositivos da rede devem ser alteradas a cada rotina de manutenção preventiva, conforme período estabelecido na planilha de eventos da rede, e imediatamente a qualquer suspeita de vazamento ou quebra.

7. As senhas dos usuários cadastrados no AD não devem ter um período de expiração, e os usuários devem ter autonomia para alterar suas respectivas senhas a qualquer momento.

8. A autenticação de dois fatores (2FA) deve ser configurada, sempre que possível, nos servidores e aplicações da rede.

GLOSSÁRIO

Active Directory: É um serviço de diretório desenvolvido pela Microsoft para redes de domínio Windows.

Clonagem: Processo de substituição dos dados do disco rígido pelos dados de uma imagem de disco criada a partir de outro computador de mesmo modelo, pré-configurado e homologado de acordo ao documento correspondente da **DPT**.

DMZ: Zona “desmilitarizada”. Seguimento da rede local específico para conexão de dispositivos que podem ser acessados através da internet via um endereço IP público.

DPT: A **documentação de procedimentos técnicos** é um conjunto de documentos que estabelecem as ações para implantar, configurar e gerenciar os recursos e serviços de TI do campus.

Mudanças: Alterações físicas ou lógicas dos recursos ou serviços de TI já estabelecidos.

Projetos: Processo de implantação de novos recursos ou serviços de TI.

Problemas: Erros ou falhas no funcionamento dos recursos ou serviços de TI já estabelecidos.

VM: Virtual Machines – Máquinas Virtuais.