EDUCAÇÃO QUE

aproxima

Plano de ação
Segurança da Informação

EDITORA Opet

Gerenciamento de Configuração

- **Atividade 1:** Realizar ajustes no procedimento com base na análise dos resultados.
- **Atividade 2:** Implementar melhorias contínuas no processo de gerenciamento de configuração.
- **Responsável**: Gerência

- **Atividade 1:** Realizar uma revisão abrangente do atual procedimento de gerenciamento de configuração.
- **Atividade 2:** Identificar metas claras para a padronização da infraestrutura de hardware e software.
- **Responsáveis:** Suporte e Governança de TI.

- **Atividade 1:** Avaliar a eficácia do novo procedimento de gerenciamento de configuração.
- **Atividade 2:** Comparar a infraestrutura atual com as metas estabelecidas para identificar desvios.
- **Responsável:** Suporte de TI

- **Atividade 1:** Implementar o procedimento de gerenciamento de configuração conforme revisado.
- **Atividade 2:** Iniciar o processo de padronização da infraestrutura, incluindo hardware e software.

- **Responsáveis:** Suporte

Primeiros passos:

- Criar relatório revisando o atual procedimento de gerenciamento de configuração, sugerindo melhorias no processo e estruturando padrões de hardware para cada cargo de acordo com a necessidade.

- Estabelecer metas e estrutura-las em: padronização de Sistema Operacional, Hardware, controle de acesso, padronizações de ferramentas (Office 365), Backup e Recuperação.

- Robustecer o Easy Inventory

Procedimentos Operacionais de Hardening:

- **Atividade 1**: Realizar ajustes nos procedimentos de hardening com base nas análises.
- **Atividade 2:** Atualizar continuamente os procedimentos para enfrentar novas ameaças.
- **Responsável**: Gerência e infraestrutura

- **Atividade 1**: Definir metas específicas para fortalecimento da segurança por meio do hardening.
- **Atividade 2**: Identificar ameaças potenciais e mapear os processos de hardening necessários.
- **Responsáveis:** Infraestrutura

- **Atividade 1:** Avaliar a eficácia dos procedimentos de hardening implementados.
- **Atividade 2:** Analisar relatórios de vigilância para verificar a segurança do sistema.
- **Responsável:** Gerência

- **Atividade 1:** Implementar procedimentos de hardening conforme as diretrizes estabelecidas.
- **Atividade 2:** Monitorar continuamente possíveis ameaças e ataques ao sistema.

- **Responsáveis:** Governança de TI

Primeiros passos:

- Enumerar todos os ativos de hardware e software na infraestrutura, incluindo servidores, estações de trabalho e smartphone.

- Criar um relatório avaliando todas as ameaças em potenciais e as vulnerabilidades nos sistemas. O relatório será utilizado para priorizar os temas mais críticos.

- Criar políticas de segurança específicas para o ambiente da Editora Opet. As políticas devem abordar temas como: controle de acesso, gerenciamento de contas e políticas de senhas.

Controle de Softwares Maliciosos

- **Atividade 1**: Realizar ajustes na proteção conforme necessário.
- **Atividade 2:** Atualizar continuamente os softwares de acordo com as melhores práticas.
- **Responsável**: Gerência e infraestrutura

- **Atividade 1:** Estabelecer metas claras para proteção contra softwares maliciosos.
- **Atividade 2:** Identificar softwares essenciais para o dia a dia
- **Responsáveis:** Suporte

- **Atividade 1:** Avaliar a eficácia da proteção contra softwares maliciosos.
- **Atividade 2:** Verificar a conformidade com as recomendações dos fabricantes.
- **Responsável:** Suporte

- **Atividade 1:** Implementar softwares de proteção centralizados e homologados.
- **Atividade 2:** Garantir a atualização automática e centralizada dos softwares prioritários.

- **Responsáveis:** Suporte

Primeiros passos:

- Avaliar todos os endpoints do parque, principalmente os inativos. Precisamos garantir que todas as estações de trabalho e servidores tenham a solução antivírus instalada e comunicando frequentemente com o antivírus.

- Realizar treinamentos com a BitDefender para atuar no console, a partir do treinamento realizar monitoramento constante para identificar comportamentos suspeitos de softwares maliciosos.

- Criar uma lista com os principais softwares utilizados pela área de negócio e homologá-los.

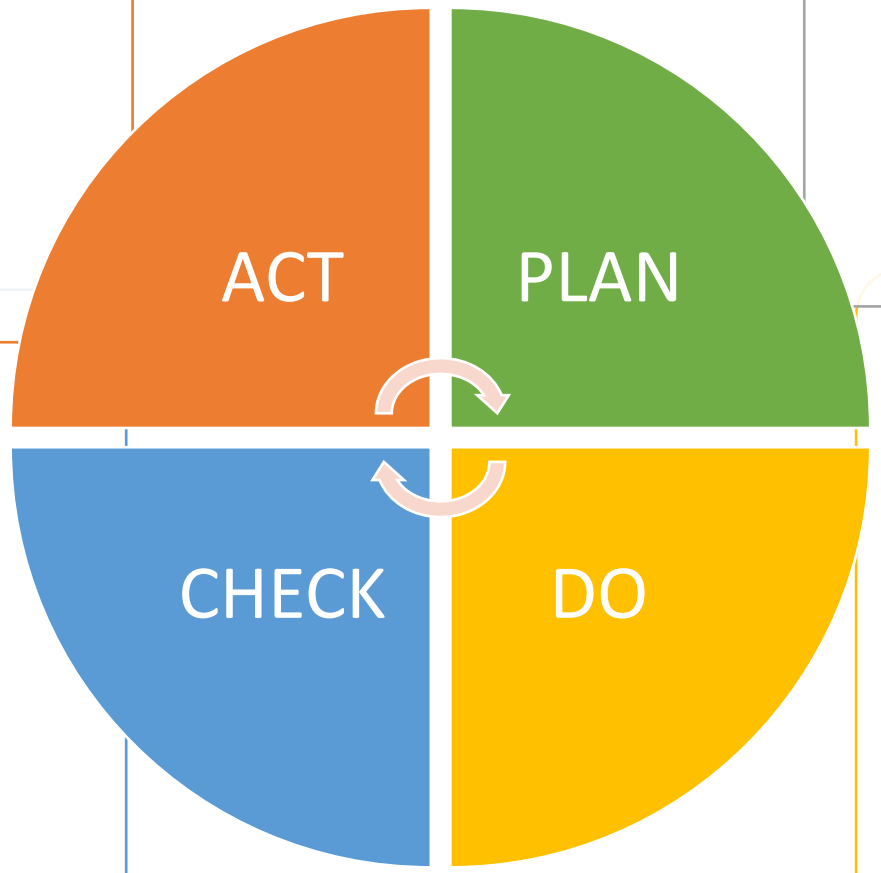
Configuração de Softwares por Perfil de Usuário

Primeiros passos:

- Definir o perfil de acesso de acordo com a área: Administrativo, BI, Desenvolvimento, Suporte, Financeiro, RH e afins.

- Avaliar com as áreas os principais softwares utilizados e lista-los. A partir da lista, identificar quais apresentam riscos de vulnerabilidade ou não.

Desativação do Administrador Local em Todos os Equipamentos



- Agir com base nos resultados da verificação e monitoramento.
- Realizar ajustes necessários no processo de desativação, se necessário.
- Atualizar procedimentos de treinamento conforme feedback recebido.
- Planejar revisões periódicas do processo para garantir a eficácia contínua.

- **Responsável**: Gerência e Suporte

- Identificar equipamentos com contas de administrador local ativas.
- Comunicar internamente sobre a desativação, esclarecendo motivos.
- Realizar backup de dados críticos nos equipamentos.
- Estabelecer cronograma para desativação remota/manual.

- **Responsável:** Suporte

- Verificar se todas as contas de administrador local foram desativadas.
- Monitorar continuamente para identificar tentativas de reativação.
- Avaliar a eficácia do treinamento e comunicação interna.
- Analisar o sistema de monitoramento para detecção de eventos anômalos.

- **Responsável:** Suporte e Gerência

- Executar o levantamento e inventário dos equipamentos.
- Comunicar internamente sobre a desativação e providenciar treinamento.
- Realizar backup de dados críticos.
- Desativar contas de administrador local de forma remota ou manual.
- Validar efetividade da desativação.

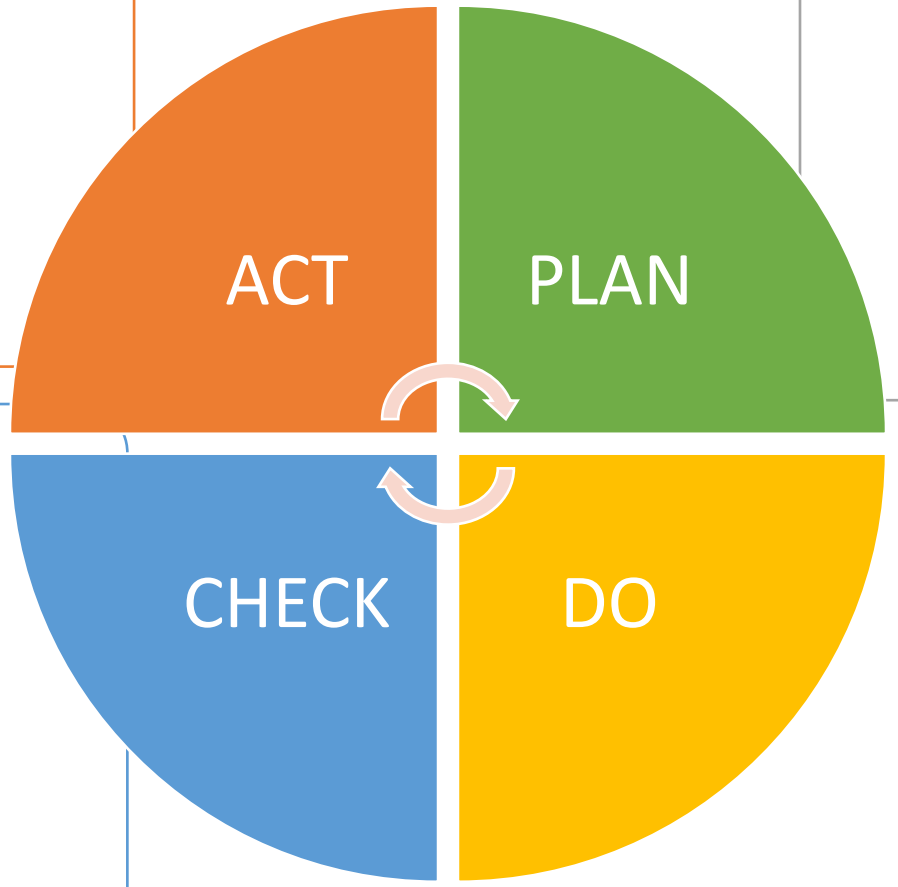
Primeiros passos:

- Identificar todas as máquinas que possuem administrador local e comunicar internamente sobre a desativação, esclarecendo motivos.
- Realizar backup de dados críticos nos equipamentos
- Estabelecer cronograma para desativação remota/manual.

Habilitar Logs de Auditoria nas Estações e no Domínio

- Identificar as políticas de auditoria necessárias para atender aos requisitos de segurança.
- Definir quais eventos devem ser registrados nos logs de auditoria.
- Comunicar internamente sobre a implementação das políticas de auditoria.
- Estabelecer um cronograma para a implementação das políticas de auditoria.

- **Responsável:** Suporte



- Configurar as políticas de auditoria nas estações de trabalho e nos servidores do domínio.
- Verificar se as configurações estão corretas e de acordo com as políticas estabelecidas.
- Realizar testes para garantir que os logs estão sendo gerados conforme o esperado.
- Comunicar internamente sobre a conclusão da implementação.

- Monitorar continuamente os logs de auditoria para identificar eventos relevantes.
- Verificar se os logs estão fornecendo informações úteis para a segurança da rede.
- Avaliar se houve alguma interrupção nos sistemas devido à implementação.

- **Responsável:** Suporte

- Agir com base nas informações fornecidas pelos logs de auditoria.
- Realizar ajustes nas políticas de auditoria, se necessário.
- Aprimorar os procedimentos de monitoramento e revisão dos logs.
- Planejar atualizações regulares nas políticas de auditoria em resposta às mudanças nas necessidades de segurança

- **Responsável**: Gerência e Suporte

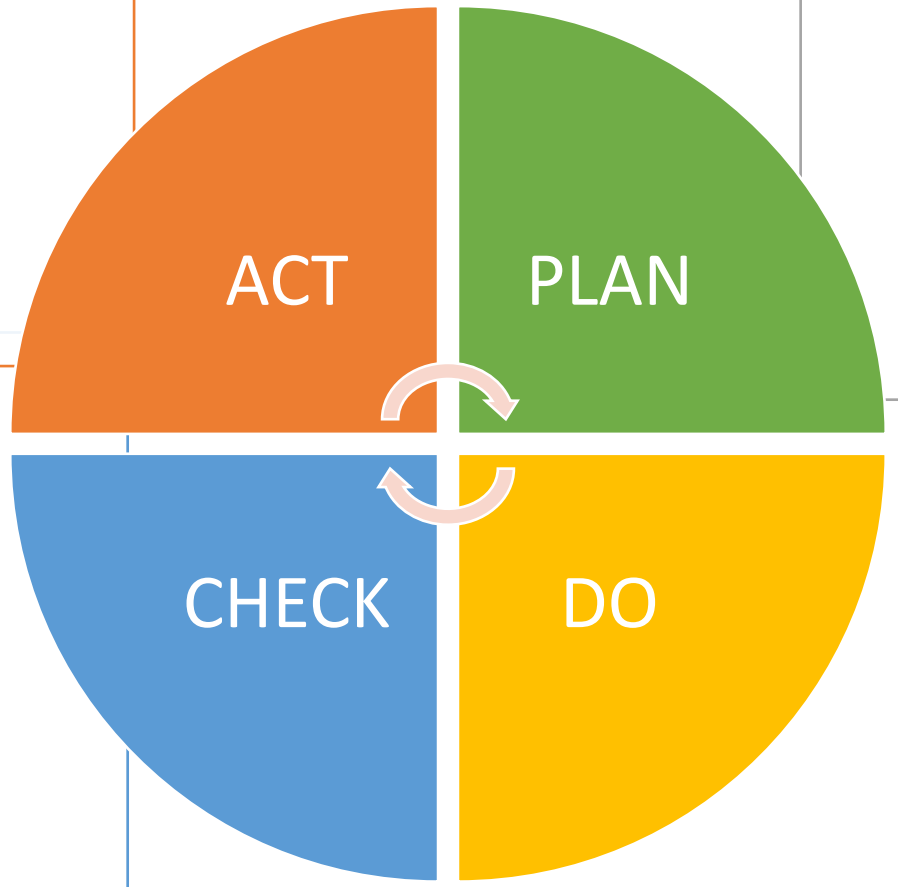
Primeiros passos:

Criar as políticas de auditoria necessárias para atender aos requisitos.

Habilitar os seguintes logs para monitorar:

- Tentativas de insucesso de logon
- Logon /logoff
- Gerenciamento de conta
- Acesso aos sistemas

Gestão Contínua de Vulnerabilidades



- Agir com base nos resultados das verificações e relatórios de vulnerabilidades.
- Realizar ajustes nas políticas e procedimentos, se necessário.
- Aprimorar a comunicação interna sobre as ações de gestão de vulnerabilidades.
- Planejar atualizações regulares nas políticas e procedimentos em resposta às mudanças nas ameaças e tecnologias.

- **Responsável**: Gerência e Suporte

- Identificar os sistemas operacionais e softwares existentes nos equipamentos.
- Estabelecer um sistema de gerenciamento de patches para controle de versionamento.
- Definir procedimentos para verificar e atualizar vulnerabilidades de forma automática e proativa.
- Criar um cronograma para as verificações e atualizações regulares.

- **Responsável:** Suporte

- Monitorar continuamente os relatórios de varredura de vulnerabilidades.
- Avaliar a eficácia do sistema de gerenciamento de patches.
- Verificar se as atualizações estão sendo aplicadas de maneira fluida e sem interrupções.
- Analisar se as ações estão alinhadas com as metas de segurança estabelecidas.

- **Responsável:** Suporte

- Realizar varreduras de vulnerabilidades em sistemas operacionais e softwares instalados.
- Implementar o sistema de gerenciamento de patches para atualização automática e proativa.
- Comunicar internamente sobre as ações em andamento.
- Criar procedimentos para garantir a execução eficiente das verificações e atualizações.

Primeiros passos:

Identificar os sistemas operacionais e softwares existentes nos equipamentos.

Implementar um sistema de gerenciamento de patchs (verificação e atualização) para o controle de versionamento que cubra tanto sistemas operacionais quanto softwares instalados nos dispositivos da organização. Isso permite a instalação de atualizações de correção de vulnerabilidade de forma automática, fluida e proativa.

Considerar os seguintes softwares prioritariamente:

- Windows – atualização automática
- Antivírus / Anti-malware – atualização automática e centralizada
- Ferramentas de apoio em geral (Office, Acrobat, Browsers, entre outros)
- Clientes – Sistemas, aplicativos, e-mails, nuvem

EDITORA Opet

EDITORA Opet

Opet Soluções Educacionais

Sefe
Sistema Educacional Família e Escola

www.editoraopet.com.br