


Plano de melhorias – Sistema de Segurança da Informação	
Projeto de melhorias	

Controle de Versões			
Versão	Data	Autor	Notas da Revisão
01	11/05/2023	Leandro Guido	Finalização da v.01

Sumário

1	Objetivos deste documento	1
2	Melhoria contínua	2
3	Melhorias e implementação	Erro! Indicador não definido.
4	Segurança da informação	Erro! Indicador não definido.
5	Documentação	Erro! Indicador não definido.


1 Objetivos deste documento

Situação inicial: Controle e documentação da tecnologia e segurança da informação.

Objetivo geral: Controlar, documentar e implementar.

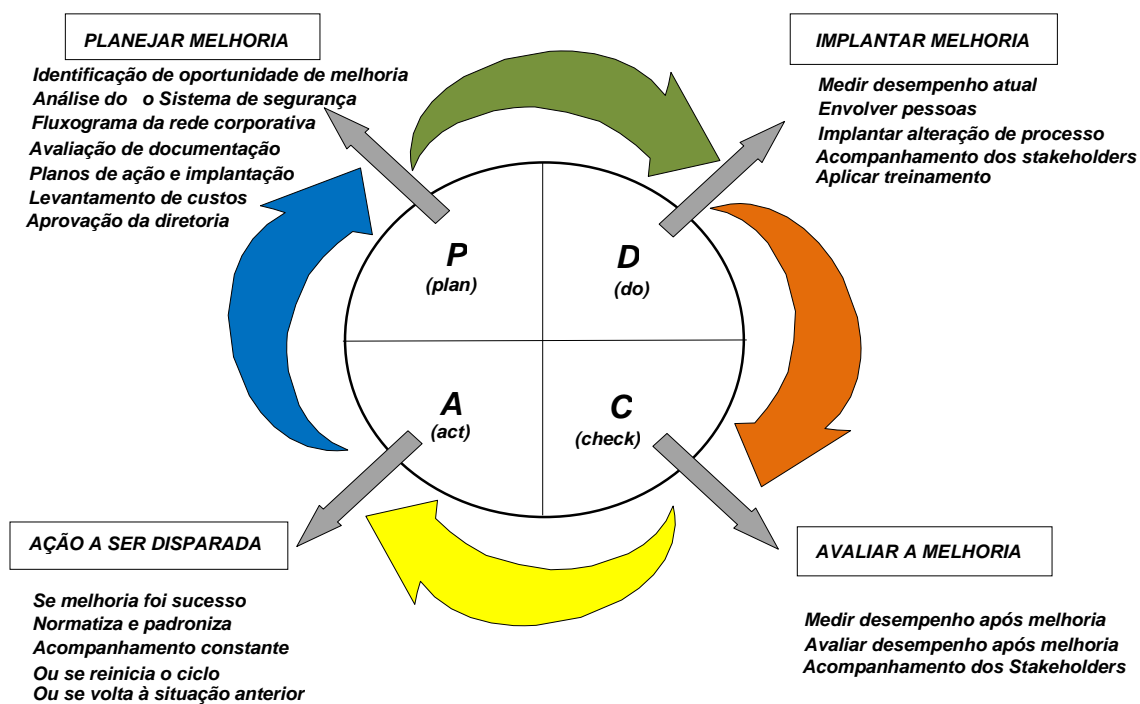
Objetivos específicos:


- Documentação e proteção;
- Criar documentações e procedimentos;
- Implementar procedimentos;
- Controle de Segurança da Informação baseado nas normas 27001;
- Treinamento;
- Conscientização de proteção e segurança da informação corporativa

Plano de melhorias – Sistema de Segurança da Informação	
Projeto de melhorias	

2 Melhoria contínua

O Plano de melhorias no processo baseia-se no ciclo PDCA conforme figura abaixo:



Plano de melhorias – Sistema de Segurança da Informação	
Projeto de melhorias	


3 Melhorias e implementação

A finalidade do presente plano de melhorias é garantir a eficiência, melhorias, implementação de controle desde a sua criação das normas e documentação até implementar no ambiente corporativo, além de implementar, orientar e conscientizar.

Toda a melhoria de segurança da informação se dará por implementar proteção em servidores, documentação, orientação e conscientização dos usuários.

Os processos relacionados aos produtos/serviços do projeto estão descritos abaixo:

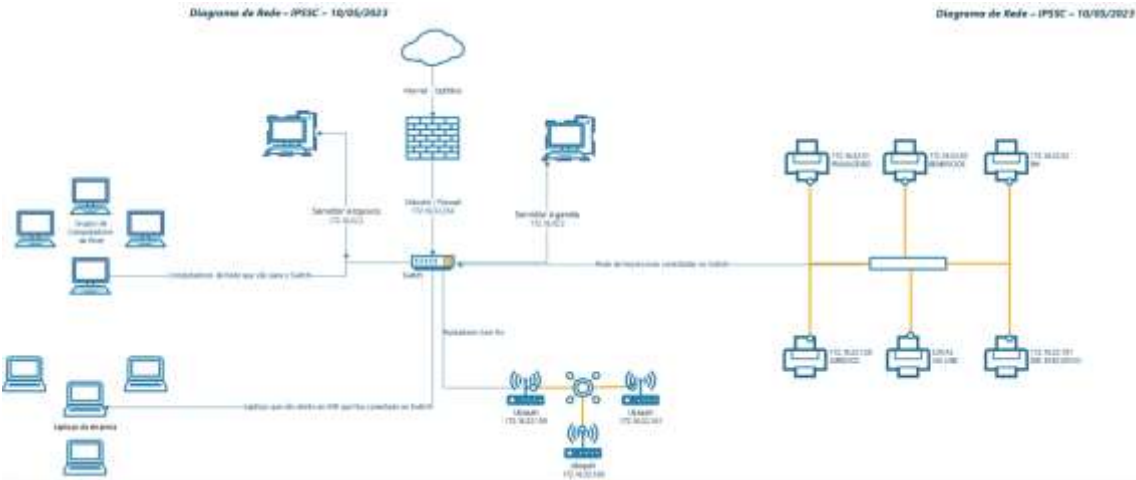
<u>Processo</u>	<u>Finalidade</u>	<u>Problema</u>	<u>Solução</u>
Segurança	Controle de informação	Não existe controle de informação.	Implementar documentação e sistemas de segurança
Segurança	Controle de acesso dos dados	Acesso a informação aberta e sem controle de quem acessa e se houve alterações	Implementar Active directory na rede e controlar acessos e controles de usuários
Gestão e segurança da informação	Controlar, monitorar, documentar e proteger	Não tem controle via pendrive de acesso e pode ser copiado e transferida informações	Criar um controle via GPO (Group Policy Organization) A fim de bloquear funções para que sejam roubadas e ou transmitidas a terceiros sem ordem.
Defesa Cibernética	Proteger ambientes corporativo de hackers nocivos	Não possui antivírus corporativo e nem backup fora do ambiente corporativo	Necessário fazer análise de vulnerabilidades e ataques de intrusão afim de identificar brechas e ter backup em nuvem

Plano de melhorias – Sistema de Segurança da Informação	
Projeto de melhorias	


4 Segurança da informação

Tendo a Segurança da informação no ambiente, será possível, controlar os ativos, ataques, proteção aos usuários, proteção sob o ambiente corporativo, tirando a exposição ao ambiente externo e roubo de informação.

Fluxograma do ambiente corporativo hoje no IPSSC.



<u>Processo</u>	<u>Finalidade</u>	<u>Problema</u>	<u>Solução</u>
Controle	Proteger contra ameaças externas	Sem mecanismos de defesa	Adquirir antivírus corporativo

Plano de melhorias – Sistema de Segurança da Informação	
Projeto de melhorias	

5 Documentação

A documentação ajudará na implementação e consciência do usuário que terá acesso e ciência do que poderá ou não fazer dentro do ambiente corporativo e em caso de vazamento de dados e perda de dados, poderá responder civil ou criminalmente pelo dano causado a empresa.