Faculdade Senac Goiás

Ismael Derick Brito Cardoso

João Vitor Vieira Felicio

Rone Augusto Oliveira Jacob

Segurança da Informação

2019

Política de controle de acesso lógico de hardware e software

1. Apresentação

Este documento e seus anexos definem as normas a serem seguidas para acesso ao sistema desenvolvido no componente curricular Programação com Frameworks.

A elaboração e a atualização deste documento são de responsabilidade da equipe elaboradora do programa desenvolvido para o Projeto Integrador da turma de Gestão da Tecnologia da Informação Modulo V.

2. Escopo

Este documento define as regras e procedimentos gerais para o acesso lógico aos sistemas e ativos de informação. As regras específicas, de acordo com o tema, estarão declaradas nos anexos deste documento, os quais abordarão os seguintes pontos:

- Recursos (Ativos) necessários para manter a confiabilidade;
- Análise de Riscos
- Disponibilidade e autenticidade no acesso ao sistema.
- Política de controle de acesso.

Data de Criação: 04/06/2019 Grupo três do projeto integrador da turma de Gestão da Tecnologia da Informação Modulo V.

3. Público-Alvo

As regras aqui dispostas aplicam-se a todos e a qualquer pessoa ou entidade que interaja com o programa elaborado no componente curricular Programação com Frameworks.

4. Objetivos

Definir regras claras e objetivas para o acesso lógico a informações, serviços e recursos de TI.

5. Disposições Finais

- Este documento e seus anexos devem ser amplamente divulgados para todos os alunos e professores na apresentação do projeto integrador.

- Este documento e seus anexos deverão estar disponíveis, para acesso ou download, a qualquer tempo, através dos meios adequados.

Anexo I

Recursos (Ativos) necessários para manter a confiabilidade

1) Apresentação

Neste anexo serão listados todos os recursos necessários para manter a confiabilidade.

2) Lista de Todos os Recursos

a) Recursos de Hardware
- Servidores
- Switches
- Roteadores
- Firewall

b) Recursos de Software
- Banco de Dados
- Serviço de Antivírus
- Sistema de Hospedagem web

3) Objetivos

Apresentar os recursos necessários que devem manter a confiabilidade.

4) Disposições Finais

- Recursos de Hardwares e softwares disponíveis para a equipe de TI que deve manter a confiabilidade.

- Estes ativos de software e hardware deverão estar disponíveis, para acesso a equipe de TI, a qualquer tempo, através dos meios adequados.

Anexo II

Análise de Riscos

1) Apresentação

Apresentamos a vocês às vulnerabilidades, ameaças e impactos.

2) Quadro que mostra às vulnerabilidades, ameaças e impactos dos hardwares e Softwares

Hardwares

Ativos	Vulnerabilidades	Ameaças	Impactos
Servidores	Sistema operacional, Configuração do Servidor, Senhas Fracas e Falta de Atualização	Lentidão, vírus, Senhas Expostas e Malwares	Prejuízo na confiabilidade, financeiro, Hardwares do Servidor e travamentos
Switches	Localização indevida	Interceptação de pacotes, Acidentes, Acesso indevido	Falha de conexão a Internet
Roteadores	Ataques a roteadores, senhas fracas	Acesso a rede e informações	Não acesso a rede
Firewall	Portas abertas	Invasão	Furto de informações

Software

Ativos	Vulnerabilidades	Ameaças	Impactos
Banco de Dados	Senhas Fraca, Privilégios excessivos de usuários e grupos, Funcionalidades desnecessárias habilitadas no banco de dados, Dados sensíveis não criptografados	Usuários com privilégios desnecessários, perca de dados, invasão	confiabilidade, financeiro, perca de dados e alteração indesejada
Serviços de Antivírus	Mal configuração, desatualizado	Vírus e Malwares	Perca de dados
Sistema de Hospedagem	Falhas na injeção	vulnerabilidades dos dados e perca de dados	perca das informações e prejuízo financeiro

Anexo III

Disponibilidade e autenticidade no acesso ao sistema

1) Apresentação

Este documento é parte da Política de Controle de Acesso Lógico. Os integrados do Projeto Integrador deverão tê-lo à disposição, citá-lo e disponibilizá-lo para os usuários sempre que forem questionados com relação aos procedimentos adotados para a criação de contas.

2) Disposições Gerais

- Na hipótese de o Sistema de Informação possuir módulo específico para a manutenção e criação de contas, habilitado para uso do Gestor do Sistema, a responsabilidade pela criação e manutenção de contas é de exclusiva responsabilidade deste. Portanto, o Gestor de Sistema de Informação deverá zelar pela base de usuários de sistema de forma que somente pessoas autorizadas tenham acesso ao sistema.

- Para o cadastro no sistema devem fornece todos os dados necessários para a realização do cadastro e para a alteração ou exclusão de contas no sistema.

- A equipe de TI ou servidor designado para controlar os acessos ao Sistema de Informação ficará responsável por providenciar a assinatura pelo usuário de Termo de Responsabilidade, atestando estar ciente dos direitos, responsabilidades e possíveis sanções pelo uso indevido da conta do sistema.

- É responsabilidade do Gestor do Sistema de Informação solicitar o cancelamento da conta de acesso ao sistema ou a alteração de perfil.

3) Disposições Finais

- Os dados necessários ao acesso ao sistema são definidos pelo Gestor de Sistema de Informação e serão informadas ao cliente pelo programa quando for criar a conta.
- As senhas iniciais criadas durante o cadastro de contas novas e todas as senhas reinicializadas por solicitação do titular deverão ter prazo de expiração de no máximo 48 horas.

.

Anexo VI

Política de Controle de acesso

1) Apresentação

Este documento é parte da Política de Controle de Acesso Lógico. Os integrados do Projeto Integrador deverão tê-lo à disposição, citá-lo e disponibilizá-lo para os usuários sempre que forem questionados com relação aos procedimentos adotados para o controle de acesso a Hardwares e Softwares.

2) Disposições Gerais

- As exigências a seguir descritas atingem todos os usuários do sistema
- Somente a equipe de TI deve ter o acesso ao Ativos do programa e dos hardwares

3) Disposições Finais

.

- Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de hardwares que são exclusivos para o programa.
- No caso acima, os atos praticados serão de responsabilidade de todos os envolvidos, estando sujeitos às sanções administrativas e penais cabíveis, tanto o titular das credenciais quanto aquele que as utilizar indevidamente.