

**Faculdade de Tecnologia SENAC Goiás**

**Gestão da Tecnologia da Informação**

**Segurança da Informação**

**ATIVOS CRÍTICOS DE RISCO E AMEAÇAS**

**Alunos:** Antônio Bueno de Camargo  
Hudson Rodrigues

Iury Neres Santana  
Ivan Luís

**Junho - 2018**

# ATIVOS CRÍTICOS DE RISCO

|  |  |  |  |
| --- | --- | --- | --- |
| **Ativos** | **Vulnerabilidades** | **Ameaças** | **Impactos** |
| Servidor web | Erro de configuração de IP | Falta de internet | Funcionamento externo da loja |
| Configuração do firewall / portas de serviços abertas | Ataque de negação de serviço | Indisponibilidade do servidor web |
| Implantação de um nobreak | Falta de Eletricidade | Funcionamento do Servidor |
| Hardwares Substitutos | Queima de Hardwares | Funcionamento do Servidor |
| Servidor Banco de Dados | Erro de configuração do servidor | SQL Injection | Confiabilidade dos dados |
| Malware | Comprometimento das informações | Perca de dados |
| Backups desprotegidos | Exposição de Mídia Storage | Confiabilidade dos dados |
| Configuração do firewall / portas de serviços abertas | Ataque de negação de serviço | Indisponibilidade do servidor de banco de dados |
| Implantação de um nobreak | Falta de Eletricidade | Funcionamento do Servidor |
| Hardwares Substitutos | Queima de Hardwares | Funcionamento do Servidor |
| Switch | Switches Substitutos | Queima do switch | Comunicação com os servidores |
| Implantação de um nobreak | Falta de Eletricidade | Comunicação com os servidores |
| Excesso de requisições | CAM Table overflow attack | Comunicação com os servidores |
| Roteador | Roteador Substitutos | Queima do roteador | Indisponibilidade de internet |
| Servidor Firewall | Implantação de um nobreak | Falta de Eletricidade | Funcionamento do Servidor firewall |
| Hardwares Substitutos | Queima de Hardwares | Funcionamento do Servidor firewall |
| Configuração do IPTABLES | Acesso não autorizado | Confiabilidade |
| Sistema operacional | Trojan Horse | Libera portas | Acesso indevido |
| Perca de arquivos | queima do Hd | Comprometimento dos arquivos |
| Loja Virtual | Configuração do firewall / portas de serviços abertas | Ataque de negação de serviço | Indisponibilidade do servidor web |
| Configuração do Spring MVC | Acesso não autorizado | Confiabilidade |

# RISCOS INERENTES AOS ATIVOS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Análises de Impactos** | | | | | |
| **1** | | Irrelevante | | | |
| **2** | | Efeito Pouco significativo | | | |
| **3** | | Efeito Médio Significativo | | | |
| **4** | | Efeito Alto Significativo | | | |
| **5** | | Perdas Financeiras | | | |
| **6** | | Efeito Desastrosos | | | |
| **Tabela de Probabilidades** | | | | |
| **PONTOS** | **AVALIAÇÃO** | | **PROBABILIDADES** | **ATRIBUTOS** |
| **1** | Probabilidade quase nula | | <= 10% | Eventos somente ocorrerá em circunstâncias excepcionais |
| **2** | não provável | | <=30% | Evento não é provável, mas pode ocorrer |
| **3** | Provável | | <= 60% | Evento que pode ocorrer provavelmente |
| **4** | Muito provável | | <= 70% | Evento que pode ocorrer na maioria das circunstâncias |
| **5** | Esperado | | <= 90% | Evento é esperado que ocorra no futuro próximo |
| **6** | Muito esperado | | > 90% | Evento com muita convicção de acorrer |

|  |  |  |
| --- | --- | --- |
| **Tabela de impactos** | | |
| **PONTOS** | **AVALIAÇÃO** | **ATRIBUTOS** |
| **1** | limitado | Impacto limitado nas operações, em regulamentos ou responsabilidades. Questões que podem ser delegadas para colaboradores |
| **2** | baixo | baixo impacto para algumas atividade |
| **3** | moderado | impacto moderado para as operações |
| **4** | elevado | Alto impacto para as operações. Significantes impactos para a reputação da organização |
| **5** | alto | impacto significante para as operações estratégicas, financeiras que impedem a continuação normal das operações |
| **6** | Muito alto | impacto significante para as operações estratégicas, financeira e operacional podendo para a empresa |

|  |  |  |
| --- | --- | --- |
| **Matriz de Ameaças** | | |
| Ameaças | impactos | probabilidade |
| falta de internet | 4-5-6 | <= 90% |
| ataque de negação de serviço | 5-6 | <= 90% |
| falta de eletricidade | 6 | > 90% |
| Queima de Hardware | 2-3 | <= 60% |
| SQL Injection | 4 | <= 70% |
| Comprometimento de informações | 2-3-4-5 | <= 90% |
| Exposição de mídia Storage | 1-2 | <= 30% |
| CAM Table Overflow Attack | 3-4 | <= 70% |
| acesso não autorizado | 4-6 | <= 90% |
| porta de serviços aberta | 2-3 | <= 60% |

# MEDIDAS PARA CONTROLE DOS RISCOS

Para melhor funcionamento da Loja Virtual vamos adotar medidas para controle dos riscos, políticas de manutenção, reposição dos equipamentos que completam a área hardware da empresa. Esses equipamentos merecem uma observação e um planejamento na disposição deles dentro da área de trabalho da empresa, para evitar acidentes naturais que podem comprometer a integridade e a segurança do equipamento.

Os riscos que a área de software da empresa apresenta, em geral, se trata de  
dados e informações. O maneja de informações sensíveis devem seguir conforme a  
política de segurança, detalhando medidas especificas para cada software. Para tanto,  
é necessário adotar medidas de segurança que podem ser descritas em um documento  
e apresentadas para todos os funcionários da organização.

# POLÍTICAS DE SENHAS

* Será adotado um padrão de prazo de validade das senhas (30 dias), que obriga o usuário a renovar as suas senhas nesse período;
* Proibir a repetição de caracteres. Por exemplo: Se a senha era ‘root123’ a próxima senha deverá ser pelo menos 50% diferente da antiga;
* Utilização de números e letras maiúsculas e minúsculas e caracteres especiais;
* Certificar que não tenha ninguém observando no momento em que está digitando a senha;
* Não fornecer a senha a terceiros em hipótese alguma.

# SERVIDOR WEB

* O uso será restrito, somente pessoas autorizadas podem utiliza-lo;
* A manutenção será diária para garantir o melhor funcionamento;
* Um sistema de senhas para utiliza-lo será implantado;
* O local dos servidores deverá ser reservado, sem muita circulação de pessoas;
* O local deverá ser refrigerado adequadamente;
* Deverá haver sempre um hardware substituto;
* Deverá haver um nobreak para o servidor em caso de falta de eletricidade;
* Realização de backup a cada atualização.

# SERVIDOR BANCO DE DADOS

* O uso será restrito, somente especialistas podem utiliza-lo;
* A manutenção será diária para garantir o melhor funcionamento;
* Realização de Backup diário;
* Um sistema de senhas para utiliza-lo será implantado;
* O local dos servidores deverá ser reservado, sem muita circulação de pessoas;
* O local deverá ser refrigerado adequadamente;
* Deverá haver sempre um hardware substituto para troca imediata;
* Deverá haver um nobreak para o servidor em caso de falta de eletricidade.

# SERVIDOR FIREWALL

* O uso será restrito, somente pessoas autorizadas podem utiliza-lo;
* A manutenção será semanalmente para garantir o melhor funcionamento;
* Um sistema de senhas para utiliza-lo será implantado;
* O local dos servidores deverá ser reservado, sem muita circulação de pessoas;
* O local deverá ser refrigerado adequadamente;
* Deverá haver sempre um hardware substituto para troca imediata;
* Deverá haver um nobreak para o servidor em caso de falta de eletricidade;
* Realização de backup a cada atualização.

# SWITCHES

* Configuração somente por pessoa especializada, para evitar CAM Table Overflow Attack;
* Deverá haver sempre um hardware substituto;
* O local de instalação deverá ser sempre em um rack com ventilação, sem muita circulação de pessoas;
* Deverá haver um nobreak para o servidor em caso de falta de eletricidade.

# ROTEADOR

* Roteador substituto para substituição imediata em caso de defeito ou queima do equipamento;
* Link de internet para redundância;
* A configuração deve ser feita por pessoa especializada, em balanceamento de link de internet e controle de banda;
* O local de instalação deverá ser em uma sala especifica com segurança, dentro de um rack, com ventilação adequada;
* Deverá haver um nobreak para o servidor em caso de falta de eletricidade.

# SISTEMA OPERACIONAL

* Utilização de antivírus para proteção do sistema;
* Bloqueio de sites feito pelo firewall;
* Proibição de acesso de sites de rede sociais, com exceção os que necessitem desses sites como ferramenta de trabalho;
* Backup dos arquivos do sistema operacional;
* O sistema operacional será acessado somente por usuários autorizados;
* A instalação de softwares será de responsabilidade dos usuários com permissão de administradores.

# LOJA VIRTUAL

* Backup do sistema da loja virtual a cada atualização;
* O usuário administrador poderá ver todas as compras pelos outros usuários, atualizar status de pagamento, cadastrar, alterar ou excluir forma de pagamento, unidade de medida, usuários, produtos e sua senha;
* O usuário cliente poderá apenas realizar compras, ver suas vendas e alterar sua senha;
* O usuário público poderá apenas ver a vitrine da loja, não podendo fazer nada sem se cadastrar primeiro.