

**Faculdade de Tecnologia SENAC Goiás**

**Gestão da Tecnologia da Informação**

**Segurança da Informação**

**?????**

**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 |

# 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