**FACULDADE DE TECNOLOGIA SENAC GOIÁS**

ALEXANDRE COSTA SANTOS

ALESSANDRO MIGUEL MANSO

DEUSAIR WELLIGNTON PEREIRA

**PROJETO INTEGRADOR**

**MODULO V**

**Gestão da Tecnologia da Informação**

**Segurança da Informação**

**Professor: Kelly Alves**

Goiânia

2018

**Sumario**

Tabela de Vulnerabilidade, Ameaças e Impactos.............................03

Análise de impactos..........................................................................04

Cálculo de Riscos..............................................................................05

Soluções para impactos.....................................................................05

Bibliografia.......................................................................................06

**Tabela de Vulnerabilidade, Ameaças e Impactos**

|  |  |  |  |
| --- | --- | --- | --- |
| **ATIVOS E RISCOS** | **VULNAREBILIDADE** | **AMEAÇAS** | **IMPACTOS** |
| Software usados na loja virtual | erro | Falha | Perda informações |
| Pessoas envolvidas | Erro humano | Falha no processo | Resultado não atingido |
| Servidor | Rotinas não processadas nos scripts | Programas e dados não atualizados | Informações repassadas do servidor desatualizadas |
| Firewall | Portas abetas com risco de invasões | Roubo de dados , acesso a informações  Privilegiadas , danos ao servidor e outros | Privacidade e base de dados em risco na de terceiros . |
| Banco de dados | Senha de acesso fácil | Facilidade de acesso de terceiros a banco de dados | Segurança dos valores , produtos e cadastros e custos comprometido |
| Internet | Instabilidade de sinal | Loja virtual não atribuir transações e confirmações de pagamentos | Perda de vendas e negociações em longa escala |
| Impressora | Defeito , de funcionamento  ( mau uso ) | Não emissão de notas fiscais para envio ao cliente via transportadoras e correios , não emissão de relatorias de confirmações de pagamentos . | Demora na entrega de compras realizadas , riscos de pagamentos não efetivados no sistema |
| computadores | Falta de anti-virus e manutenção | Vírus , sujeira nos componentes | Computador danificado , danos no  Software corrompido |
| Rotiador | Falha em sincronismo | Queda no acesso | Não acesso a rede externa |
| Proxy | Configuração errada | Acesso externo não autorizado , acesso interno não autorizado | Visualização e perda de informações a terceiros |

**Análise de impactos:**

Pode se considerar impactos em curto e longo prazo, exemplo:

* 0 – Irrelevante.
* 1 – Efeito pouco significativo.
* 2 – Sistemas não disponíveis por determinado período.
* 3 – Perdas financeiras.
* 4 – Efeitos desastrosos, sem comprometimento do negócio.
* 5 - Efeitos desastrosos, com comprometimento do negócio

|  |  |  |
| --- | --- | --- |
| **AMEAÇAS** | **IMPACTOS** | **PROBABILIDADE** |
| Falha | 4 | 80% |
| Falha no processo | 3 | 20% |
| Programas e dados não atualizados | 2 | 20% |
| Roubo de dados , acesso a informações  Privilegiadas , danos ao servidor e outros | 5 | 40% |
| Facilidade de acesso de terceiros a banco de dados | 5 | 40% |
| Loja virtual não atribuir transações e confirmações de pagamentos | 3 | 95% |
| Vírus , sujeira nos componentes | 2 | 80% |
| Queda no acesso | 4 | 60% |
| Acesso externo não autorizado , acesso interno não autorizado | 5 | 90% |

**Cálculo de Riscos**

•Riscos são calculados a partir da relação entre impacto e probabilidade de ocorrência:

•risco = impacto \* probabilidade.

•Em particular, considerando as classificações propostas para impacto e probabilidade anteriormente apresentadas, ao efetuar a multiplicação, obtém-se uma faixa de valores para o risco de 0 (nenhum risco) até 15 altíssimo

**IMPACTO \* PROBABILIDADE RISCO/PESO**

|  |  |  |
| --- | --- | --- |
| IMPACTO | PROBABILIDADE | RISCO/PESO |
| 4 | 80% | 3.2 |
| 3 | 20% | 0.6 |
| 2 | 20% | 0.4 |
| 5 | 40% | 2.0 |
| 3 | 95% | 2.75 |

NENHUMA = ATÉ 0.9

BAIXISSIMA= 1 ATÉ 1.9

BAIXO= 2 ATÉ 2.9

MÉDIO= 3 ATÉ 3.9

ALTO= 4 ATÉ 5

**Soluções para impactos**

Ações tomadas para evitar danos a empresa:

Criar rotina de revisão de processos e códigos a fim de reconhecer falhas;

Verificar postas de acesso de computadores procurando possíveis vulnerabilidades;

Verificar possibilidade de inundação no ambiente de informática e servidores;

Evitar materiais tecnológicos sem suporte (diretamente no chão);

Verificar posicionamento de material averiguando locais húmidos ou muito quentes;

Manutenção e higienização do ambiente periodicamente;

Bibliografia

<https://pt.scribd.com/doc/50809607/ITIL-v3-Fundamentos>

Conceitos aplicados em sala de aula pela professora