FACULDADE DE TECNOLOGIA SENAC GOIÁS

Gestão da Tecnologia da Informação

SEGURANÇA DA INFORMAÇÃO

GOIÂNIA, JUNHO DE 2018

Fazer uma análise de risco de ativos críticos para o sucesso do negócio, baseado no sistema de controle de acesso desenvolvido no componente Programação com Frameworks e propor medidas para controle dos riscos.

Alunos: Emanuel dos Santos Cruz
Kadmiel dos Santos Cruz
Klecio Holanda de Sousa
Vinícius de Godoy Rodrigues

Professora: Kelly Alves Martins de Lima

Ativos críticos e suas políticas

Ativos críticos são bens, seja hardware ou software, que possui um valor e uma determinada função para ser utilizado em uma empresa. Nesse projeto o uso é destinado a loja virtual. Uma política de uso deve ser feita, para adquirir o funcionamento correto e junto uma política de segurança para resguardar os bens.

A política de segurança trata apenas de questões voltadas à segurança física e lógica da informação, visando dar suporte a estratégia de negócio e plano de continuidade de negócio.

Ativos críticos utilizados na loja virtual

Classificados como **HARDWARES**:

- Computador;
- Nobreak;
- Roteador;
- Servidor;
- Switch;

Classificados como **SOFTWARES**:

- Banco de Dados;
- Domínio;
- Internet;
- Sistema de Informação da Loja;
- Sistema Operacional;

Gestão de riscos

Levantamento dos ativos críticos relacionados a tecnologias para o sucesso do negócio.

GESTÃO DE RISCO				
CATEGORIA	**ATIVOS CRÍTICOS**	**VULNERABILIDADE**	**AMEAÇAS**	**IMPACTOS**
Hardware	Computador	Poeira, software maliciosos	Desastres causados por pessoas	Mal funcionamento do computador
	Nobreak	Bateria baixa, falta de manutenção	Falha em equipamento	Falta de energia
	Roteador	Ataques	Monitoramento de tráfego na rede	Instabilidade, falha de conexão
	Servidor	Configuração incorreta de segurança	Invasão	Manutenção em configuração
	Switch	Erro de configuração	Usuários internos praticando atos ilegais	Afeta na performance da rede
Software	Banco de dados	Exposição de dados sensíveis, SQL injection	Modificação de informações	Reformulação de código SQL
	Domínio	Falha de conexão	Invasão	Queda de acessos
	Internet	Ataques maliciosos	Desastres causados por pessoas	Invulnerabilidade
	Sistema de Informação da loja	Erro de código	Códigos maliciosos	Custo e tempo em reestruturação do código
	Sistema operacional	Sistema desatualizado	Bugs dos sistemas operacionais	Compromete performance do SO

Análise de impactos

Pode considerar o impacto em curto e longo prazo. Exemplo de classificação:

- 0 - Irrelevante.
- 1 - Efeito pouco significativo.
- 2 - Sistemas não disponíveis por determinado período.
- 3 - Perdas financeiras.
- 4 - Efeitos desastrosos, sem comprometimento dos negócios.
- 5 - Efeitos desastrosos, comprometendo os negócios.

Matriz de Relacionamento

MATRIZ DE RELACIONAMENTO		
AMEAÇAS	**IMPACTO**	**PROBABILIDADE**
Erros humanos	3 e 5	85%
Instalação de hardware e software não autorizados	4	64%
Códigos maliciosos	2 e 3	50%
Bugs dos sistemas operacionais	3 e 5	85%
Invasão	3 e 5	85%
Desastres naturais	3	40%
Desastres causados por pessoas	5	80%
Falhas em equipamentos	1 e 2	20%
Sabotagem	5	80%
Grampo telefônico	4	64%
Monitoramento de tráfego na rede	2 e 4	56%
Modificação de informações	5	80%
Acesso a arquivos de senhas	3 e 5	85%
Uso de senhas frágeis	3 e 5	85%
Usuários internos praticando atos ilegais	5	80%

Tabela numérica

PROBABILIDADE	PROBABILIDADE X IMPACTO					PROBABILIDADE
5	25	20	15	10	5	5
4	20	16	12	8	4	4
3	15	12	9	6	3	3
2	10	8	6	4	2	2
1	5	4	3	2	1	1
IMPACTO	5	4	3	2	1	IMPACTO

LEGENDA	
1 A 5	BAIXO NÍVEL DE PROBABILIDADE X IMPACTO
6 A 14	NÍVEL MÉDIO DE PROBABILIDADE X IMPACTO
15 A 25	ALTO NÍVEL DE PROBABILIDADE X IMPACTO

Tabela de porcentagem

PROBABILIDADE	PROBABILIDADE X IMPACTO					PROBABILIDADE
5	100%	80%	60%	40%	20%	5
4	80%	64%	48%	32%	16%	4
3	60%	48%	36%	24%	12%	3
2	40%	32%	24%	16%	8%	2
1	20%	16%	12%	8%	4%	1
IMPACTO	5	4	3	2	1	IMPACTO

LEGENDA	
0,00% A 23,99%	BAIXO NÍVEL DE PROBABILIDADE X IMPACTO
24,00% A 59,99%	NÍVEL MÉDIO DE PROBABILIDADE X IMPACTO
60,00% A 100,00%	ALTO NÍVEL DE PROBABILIDADE X IMPACTO

Matriz de riscos inerentes aos ativos

ATIVOS CRÍTICOS	RISCO	PROBABILIDADE	IMPACTO	DESCRIÇÃO DO IMPACTO
Computador	20	4	4	Mal funcionamento do computador
Nobreak	8	2	4	Falta de energia
Roteador	12	3	4	Instabilidade, falha de conexão
Servidor	20	4	5	Manutenção em configuração
Switch	20	4	5	Afeta na performance da rede
Banco de dados	25	5	5	Reformulação de código SQL
Domínio	15	3	5	Queda de acessos
Internet	20	4	5	Invulnerabilidade
Sistema de Informação da loja	20	4	5	Custo e tempo em reestruturação do código
Sistema operacional	20	4	5	Compromete performance do SO

PROBABILIDADE
1 - Muito baixa
2 - Baixa
3 - Média
4 - Alta
5 - Muito Alta

IMPACTO
1 - Muito baixa
2 - Baixa
3 - Média
4 - Alta
5 - Muito Alta

Medidas para controle dos riscos

Todas as normas aqui estabelecidas serão seguidas à risca por todos os funcionários, parceiros e prestadores de serviços. O não comprimento dessa política acarretará em sanções administrativas, podendo ocasionar o desligamento do funcionário e demais usuários que possuem quaisquer ligações com a loja virtual de acordo com a gravidade da ocorrência.

É de grande importância conhecer e identificar os responsáveis pelo gerenciamento da segurança e estabelecer normas de aplicação de sanções resultantes de casos de inconformidade com a política elaborada, com relação às penalidades e casos de infração da política de segurança da empresa.

A política de segurança define normas, procedimentos, ferramentas e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação para garantir o controle e a segurança da informação na empresa. É formalmente o documento que dita quais são as regras aplicadas dentro da empresa para uso de recursos tecnológicos e descarte de informações.

A política de segurança define o que é e o que não é permitido em termos de segurança durante a operação de qualquer sistema ou material que contenha informações empresariais, com base na aplicação de regras que delimitam o acesso às informações. Assim, a base da política de segurança é a definição do comportamento esperado das pessoas que interagem com um sistema.

Á grosso modo pode-se afirmar que com a implantação de uma política de segurança da informação é a significativa a redução da probabilidade de ocorrência de quebra da confidencialidade, da integridade e da disponibilidade da informação, tal como a redução de danos causados por eventuais ocorrências.

Em relação a estabelecer medidas para o controle de riscos do ativos críticos são:

- Computador e Sistema Operacional:
    - Antivírus sempre atualizados;
    - Manutenção preventiva;
    - Orientação na forma de uso;
    - Instalação de softwares restritas, somente sob autorização do TI;

- Nobreak:
    - Manutenção preventiva;
    - Acesso permitido apenas ao departamento de TI;

- Roteador, servidor e switch:
    - Fazer manutenção periódica em toda a estrutura de rede, para verificar algum possível dano;
    - O uso é restrito e poderá ser feito somente com autorização prévia;
    - Observar funcionamento em tempo real, para não ocorrer instabilidade;
    - Backup diário;
    - Uso de senhas fortes;
    - Manter os equipamentos em local adequado;
    - Manter servidores atualizados;

- Banco de dados:
    - Backup dos dados;
    - Criptografar os dados com senhas fortes;

- Domínio e Internet:
    - Verificar os acessos dos usuários;
    - Verificar conexão, se não há instabilidade;

- Sistema de Informação da Loja:
    - Manter diariamente atualizada;
    - Backup diário;