Ativos Críticos e Riscos

Controle de Versões			
Versão	**Data**	**Autor**	**Notas da Revisão**
0.1	29/11/2016	Deborah Araujo Denis Ferreira Ezio Mendonça	-

Sumário

1 Ativos Críticos para o Negocio 3

2 Possíveis Riscos Aos Ativos 3

2.1 Hardware 3

2.2 Software 4

3 Gestão de Riscos e Problemas 5

3.1 Matriz de Probabilidade X Impacto 7

3.2 Matriz de Registro de Riscos 8

3.3 Matriz de Parâmetros 9

1 Ativos Críticos para o Negocio

Ativos críticos é tudo aquilo que é fundamental para o correto funcionamento da organização. Sua confidencialidade, integridade e disponibilidades devem ser prioridade, pois o acesso indevidos aos ativos, por pessoas não autorizadas, pode gerar consequências graves e irreversíveis.

No estudo de levantamentos críticos feitos na empresa Gyntech Soluções, foram identificados os seguintes pontos que necessitam de atenção:

- ✓ Hardware –
  - Estrutura de rede (cabeamentos, switch, roteadores, access point);
  - Servidores (Servidor de Arquivo, DHCP, Firewall, Web);
  - Desktops e Notebooks (Estações de Trabalho);
  - Impressoras;
  - Nobreak;
  - Dispositivos de Backup e Periféricos (PenDrives, CDs, DVDs);
- ✓ Software –
  - Acesso à internet (Link dedicado);
  - Serviço de e-mail;
  - Aplicações (IDEs, Sistemas Operacionais, Redirecionado de IP, Antivírus)
  - Banco de dados;
  - Realização de Backup em mídias distintas (HD externo, Nuvem, Fita);
  - Maquinas Virtuais;

2 Possíveis Riscos Aos Ativos

2.1 Hardware

Estrutura de rede (cabeamento, switch, roteadores, access point);

A estrutura de redes merece atenção pois os elementos a ela pertencentes garantem o acesso as informações da empresa, e podem apresentar vulnerabilidades quanto a ataques externos e mal funcionamento, além de estarem sujeitos a desgastes naturais.

Servidores (Servidor de Arquivo, DHCP, Firewall, Web);

Os servidores também são pontos vulneráveis principalmente a ataques externos feitos por hackers em busca de informações ou para derrubar o serviço.

Desktops e Notebooks (Estações de trabalho);

Desktops e Notebooks podem ser alvo de ataques e também de desgastes devido ao uso diário, e possuem uma vida útil de pouco mais de 5 anos.

Impressoras;

Dispositivos de impressora podem apresentar problemas com muita frequência de acordo com seu uso e precisam de manutenções regulares.

Nobreak;

Esse dispositivo é responsável por manter ligado outros dispositivos em casos de queda de energia e é essencial para certos tipos de negócio. Portanto sua disponibilidade e correto funcionamento é fundamental para o funcionamento de outros dispositivos.

Dispositivos de Backup e Periféricos (PenDrives, CDs, DVDs);

Os dispositivos de Backup garantem a recuperação de dados críticos para a organização, eles devem estar funcionando corretamente e ser armazenados em locais seguros.

2.2 Software

Acesso à internet (Link dedicado);

Um link dedicado é indispensável, principalmente para realização de backup em nuvem e transferência de arquivos pela rede. Os riscos que este item pode apresentar estão ligados a falhas de conexão que, dependendo da situação e do tempo decorrente, podem trazer grandes prejuízos e portanto é necessário encontrar um provedor de acesso confiável e que garanta a entrega da velocidade contratada com 100% de disponibilidade. Além de ser importante ter um planejamento para quando ocorrer alguma falha no acesso.

Serviço de e-mail;

O serviço de e-mail também merece atenção e um cuidado extra pois muitos dos documentos da empresa são enviados através deles para clientes e colaboradores. Existe a possibilidade de indisponibilidade e vazamento de informações.

Aplicações (IDEs, Sistemas Operacionais, Redirecionado de IP, Antivírus)

As aplicações e serviços, com frequência, precisam de atualizações e por conta disso podem apresentar mal funcionamento. Também é importante estar atento aos riscos de acesso indevido a itens das aplicações, múltiplas tentativas de login, invasões e inconsistência das informações.

Banco de Dados;

O Banco de Dados é, sem dúvidas, o ativo mais valioso de uma organização, nele cotem tudo que a empresa precisa para funcionar corretamente e é extremamente importante que esteja protegido de ataques e de problemas oriundos de atualizações e desastres naturais. É muito comum ocorrerem ataques para derrubar o serviço e também sequestro de dados.

Realização de Backup em mídias distintas (HD externo, Nuvem, Fita);

O backup, assim como o banco de dados, é importante e indispensável. É por meio dele que pode-se garantir a recuperabilidade dos dados e continuidade do negócio. As mídias de armazenamento podem estar sujeitas a desastres naturais, a furtos e a conter informações corrompidas.

Maquinas Virtuais;

São ferramentas importantes para realização de testes e garantem a segurança em do sistema original instalado na máquina, mesmo assim podem ser alvo de ataques e apresentam-se como um ponto vulnerável. Pode ocorrer de serem corrompidos por um desligamento indevido e nesse caso é possível que não tenha como recuperar.

3 Gestão de Riscos e Problemas

Para evitar problemas com Hardware, a empresa pode adotar medidas de utilização, manutenção e reposição de equipamentos com problemas. É também importante ter um bom planejamento de onde casa dispositivo deve estar para que acidentes naturais não venham a comprometer sua integridade e segurança. A forma e local onde cada um será guardado após o uso, onde serão instalados e o manuseio devem ser feitos da maneira adequada.

Quanto ao software, as medidas a serem adotadas podem variar muito de acordo com o propósito. No geral, quando se trata de informação, o importante é mantê-la segura, disponível e integra. Para tanto, é necessário adotar medidas de segurança que podem ser descritas em um documento e apresentadas para todos os funcionários da organização.

Proposta de Gestão de Risco

Hardware	
✓ Estrutura de rede (cabeamento, switch, roteadores, access point) ✓ Servidores (Servidor de Arquivo, DHCP, Firewall, Web) ✓ Desktops e Notebooks (Estações de trabalho) ✓ Impressoras ✓ Nobreak ✓ Dispositivos de Backup e Periféricos (PenDrives, CDs, DVDs)	Contratar serviço especializado para instalação dos equipamentos. Realizar manutenções periódica. Deverão ser contratadas empresas terceirizadas que garantam qualidade e sigilo, para realizar manutenções em todos os equipamentos.

Software	
✓ Acesso à internet (Link dedicado); ✓ Serviço de e-mail; ✓ Aplicações (IDEs, Sistemas Operacionais, Redirecionado de IP, Antivírus) ✓ Banco de dados; ✓ Realização de Backup em mídias distintas (HD externo, Nuvem, Fita); ✓ Maquinas Virtuais;	Contratar provedor de acesso confiável que garanta qualidade do serviço. Identificar os erros de desenvolvimentos e apresentar propostas de melhorias, testar periodicamente os sistemas contra invasões e criar controles de acesso para os usuários. Manter o antivírus atualizado. Fazer e Testar Backups.

3.1 Matriz de Probabilidade X Impacto

Os riscos identificados serão qualificados quanto a sua probabilidade e Impacto de ocorrência, conforme ilustra Quadro abaixo:

Probabilidade	Matriz de Probabilidade x Impacto				
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Impacto	1	2	3	4	5

Com base nas faixas de probabilidade e impacto da escala acima discriminada montou-se uma matriz. Multiplicasse o item impacto por probabilidade de ocorrência para mensurar o grau de severidade.

Conforme apresentado na Matriz de Probabilidade x Impacto:

- ✓ A cor Verde representa baixa probabilidade e impacto;
- ✓ A cor Amarela média probabilidade e impacto;
- ✓ A cor Vermelha alta probabilidade e impacto.

3.2 Matriz de Registro de Riscos

Descrição do Risco	Severidade	Probabilidade	Impacto	Descrição do Impacto	Ação	Descrição da Ação
Estrutura de rede (cabeamento, switch, roteadores, access point)	**20**	4 - Alta	5 – Muito Alto.	Problema na transferência de dados.	Prevenir	Realizar Manutenções Periódicas.
Servidores (Servidor de Arquivo, DHCP, Firewall, Web)	**20**	4 – Alta	5 – Muito Alto.	Perda de dados, riscos de invasão, Inacessibilidade.	Prevenir	Realizar Manutenções Periódicas.
Desktops e Notebooks (Estações de trabalho)	**15**	3 – Média	5 – Muito Alto.	Impossibilidade de realizar atividades importantes.	Prevenir	Realizar Manutenções Periódicas.
Impressoras	**10**	5 – Muito Alta	2 - Baixa	Não conseguir imprimir documentos.	Prevenir	Realizar Manutenções Periódicas.
Nobreak	**8**	2 – Baixa	4 - Alto	Problemas quando houver queda de energia	Prevenir	Realizar Manutenções Periódicas.
Dispositivos de Backup e Periféricos (PenDrives, CDs, DVDs)	**15**	3 – Média	5 – Muito Alto	Perda de dados.	Prevenir	Ter copias em locais diferentes.
Acesso à internet (Link dedicado);	**20**	5 – Muito Alto	4 – Alto	Perda de negociações. Impossibilidade de trabalhar.	Mitigar	Contratar serviço de qualidade.
Serviço de e-mail;	**10**	2 – Baixa	5 – Muito Alto	Vazamento de informações sigilosas, inacessibilidade.	Prevenir	Contratar serviço de qualidade.
Aplicações (IDEs, Sistemas Operacionais, Redirecionado de IP, Antivírus)	**20**	4 – Alta	5 – Muito Alta	Inacessibilidade, Perda de dados, Invasões.	Prevenir	Realizar testes, atualizações constantes, adquirir ferramentas de qualidade.
Banco de dados;	**25**	5 – Muito Alta	5 – Muito Alta	Perda de dados, sequestro de dados, inacessibilidade.	Prevenir	Adquirir suporte, realizar manutenções diárias, fazer backups.
Realização de Backup em mídias distintas (HD externo, Nuvem, Fita);	**20**	4 – Alta	5 – Muito Alta	Perda de dados, dados corrompidos.	Prevenir	Testar Backups, Armazenar em mais de uma mídia.
Maquinas Virtuais;	**16**	4 – Alta	4 – Alto	Perda de dados, dados corrompidos.	Prevenir	Ter backups, utilizar software seguro.

3.3 Matriz de Parâmetros

Legenda	Severidade	Probabilidade	Impacto	Ação
Definição	Probabilidade x Impacto	Chance de acontecer problemas.	Consequência do que pode acontecer.	O que pode ser feito.
Domínio	-	< 1 – Muito Baixa >= 1.1 - 2 – Baixa >=2.1 - 3 – Média >=3.1 - 4 – Alta >=4.1 - 5 – Muito Alta	1 – Muito Baixo 2 – Baixo 3 – Médio 4 – Alto 5 – Muito Alto	Prevenir Mitigar