**A IMPORTÂNCIA DO MONITORAMENTO PARA A MANUTENÇÃO DE UMA BOA INFRAESTRUTURA DE TI**

Jorge Emanuel Rodrigues Santos[[1]](#footnote-1), Roberto Michelan[[2]](#footnote-2)

Faculdade Paraíso do Ceará – FAPCE

Rua da Conceição, 1228 - São Miguel - CEP: 63.010-465 - Juazeiro do Norte – CE

emanuel\_bim@hotmail.com; roberto.michelan@fapce.edu.br

**RESUMO**

Atualmente as empresas olham com cuidado para seus ativos
informacionais, toda sua operação depende da infraestrutura de TI em
pleno funcionamento, bem como do acesso às informações via sistemas
ERP e demais softwares, como e-commerce, por exemplo. Quando não há
monitoramento constante e regras que atendam às políticas indicadas de
manutenção da infraestrutura de TI, pode ser que um serviço ou ativo
fique inacessível, causando grande prejuízo à organização. Com base nas boas práticas de gerenciamento de TI e de Segurança da Informação, este
estudo se mostra relevante, pois, auxiliará o setor TI a ter uma melhor
visão de todos os seus recursos, processos e ativos de informação, podendo assim alinhar a entrega de seus serviços com o negócio da empresa.

**Palavras chave:** Monitoramento, gerenciamento e infraestrutura.

**ABSTRACT**

Today companies look carefully at their assets information, all its operation depends on the IT infrastructure in operation, as well as access to information via

ERP and other software, such as e-commerce. When there is no constant monitoring and rules that comply with the stated policies of maintenance of the IT infrastructure, it may be that a service or asset inaccessible, causing great harm to the organization. Based on best practices in IT management and Information Security, this study is relevant because it will help the IT sector to have a better vision of all its resources, processes and assets of information, being able to align the delivery of its services with the business of the company.

**Key words:** Monitoring, management and infrastructure.

 **INTRODUÇÃO**

As empresas atualmente demandam uma extrema dependência dos sistemas computacionais que utilizam. Os sistemas ERP são a base dessas empresas para a tomada de decisões estratégicas. Sendo assim, para suportar esses sistemas, entra a infraestrutura de TI com os servidores de BD, servidores de arquivos e servidores de aplicação que são a base para a entrega desses serviços. A falta de conectividade com alguns desses equipamentos pode causar danos financeiros ao negócio e a sua imagem perante o mercado em que atua.

As grandes organizações, cada vez mais estão protegendo seu principal ativo, suas informações; isso se dá pela quantidade de ataques que as empresas sofrem causando um impacto negativo enorme para os seus negócios. Diante desses acontecimentos, mais empresas buscam proteger suas informações adotando práticas de gerenciamento de infraestrutura de TI afim de obterem um controle mais eficiente de hardware e software e gerenciamento de segurança da informação com o objetivo de manter suas informações mais seguras e reduzir seus custos com o alinhamento de TI ao seu negócio.

A ferramenta Zabbix é uma solução open source utilizada no mundo todo por grandes organizações, torna-se uma importante aliada para o perfeito monitoramento da infraestrutura de TI fazendo com que os profissionais dessa área entreguem serviços de qualidade e com mais eficiência mantendo os processos em funcionamento o maior tempo possível e agindo proativamente caso algo de errado possa vir a acontecer, através de manutenções preventivas dos ativos.

**1 FUNDAMENTAÇÃO TEÓRICA**

1.1 DISPONIBILIDADE DA INFORMAÇÃO

Para que as informações sejam entregues com facilidade e sempre ou quase sempre estejam disponíveis para quem desejar obtê-las, faz-se necessário uma boa infraestrutura por trás dos serviços oferecidos pela TI. A infraestrutura de TI, segundo João (2012), é composta por vários componentes como: hardware, software, redes e telecomunicação, gestão de dados, instalações e etc. estes precisam funcionar todos em conjunto para que haja uma entrega de valor para o negócio da empresa, pois, ela é a base para a disponibilidade dos dados. Esta se dá a partir da eficácia e acesso aos sistemas e ao funcionamento correto da rede, para que, quando necessário, o acesso por ela esteja em perfeito funcionamento, pois é através desses dois recursos que é possível acessar as informações.

A disponibilidade da informação determina que recursos estejam disponíveis para acesso por entidades autorizadas sempre que solicitadas, já a indisponibilidade se dá quando deixa de estar disponível quando necessitarem dela. Por exemplo, quando acontece uma queda de um servidor de banco de dados ou de uma aplicação crítica para o negócio (COELHO, 2014).

Um dos maiores desafios para os gestores de TI é a disponibilidade, pois a informação é o principal ativo de uma organização para a tomada de decisões das áreas estratégicas na tentativa de alavancar os negócios das empresas. Mas para alcançar essa disponibilidade, a infraestrutura precisa ser redundante, para quando um servidor cair o outro assumir o lugar. Ter um ambiente redundante para garantir disponibilidade, dependendo do tamanho de sua infra, sai muito caro e muitas vezes as empresas só investem nessa prevenção depois do problema acontecer e terem prejuízos, tantos financeiros como de negócios.

1.2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um dos pontos mais críticos de uma organização nos dias atuais. Pois todos dependem das informações armazenadas digitalmente para a tomada de decisões em um mercado muito competitivo. Essa informação pode estar armazenada de diferentes formas: eletronicamente, falada, enviada por correio convencional ou e-mail, impressa e etc. A informação, independente do seu formato, tem que ser protegida adequadamente contra os vários tipos de ameaças, minimizando assim impactos negativos para o negócio (COELHO, 2014).

A segurança da informação é responsável por proteger as informações, sistemas, recursos e os demais ativos contra os desastres, erros humanos, alteração, visualização e interceptações não autorizadas. Todos esses itens precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados continuamente para garantir que os objetivos do negócio e a segurança sejam alcançados dentro da empresa. Uma segurança da informação bem planejada reduz riscos, isola a organização das ameaças e vulnerabilidades e consequentemente reduz o impacto aos seus ativos. A segurança da informação é conquistada quando um conjunto adequado de controles, políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware são implementados (ABNT NBR ISO/IEC 27002:2013).

O monitoramento do ambiente de TI serve de apoio para alcançar os objetivos principais da segurança da informação. Através da análise dos dados transmitidos contra acessos indevidos verifica-se a confidencialidade, se não houver acesso indevido à informação transmitida garante-se assim a integridade e por último essa informação tem que estar sempre acessível quando solicitada para que a haja a garantia da disponibilidade.

1.3 GESTÃO DE RISCOS

Orisco é uma condição incerta ou um evento que possa vir a acontecer e prejudicar os processos críticos da empresa. Na maioria dos riscos identificados na TI sempre causam efeitos negativos para o negócio (PMBOK, 2010).

O primeiro passo de toda organização para gerenciar os riscos é a implementação de dois aspectos principais, que são: avaliação e gerenciamento dos riscos. A avaliação dos riscos é feita através da coleta de informações dos principais serviços de TI da empresa. Estas devem ser analisadas a fim de definir o quanto os seus serviços estão expostos aos riscos. A coleta dessas informações é importante pois a partir dela serão tomadas as decisões apropriadas para o tratamento dos riscos. Em seguida, depois dos riscos identificados, faz-se necessário um plano de gerenciamento dos mesmos, nesse plano serão definidas todas as ações necessárias e os responsáveis, para que, caso algum dos riscos identificados na etapa anterior venha a ocorrer, seja reestabelecido o mais rápido possível.

 O gerenciamento de riscos define-se em planejar qual abordagem dar a gestão de riscos de TI e executá-la. Como também levantar informações de como os riscos serão identificados, como a análise qualitativa será desenvolvida, como a análise quantitativa será criada, como será elaborado o plano de resposta ao risco e seu monitoramento (GOMES, 2008).

O propósito da gestão de riscos é melhorar a performance organizacional, minimizar os riscos, assegurar controles eficientes, aumentar a proteção e segurança, como também diminuir custos e alinhar a TI corretamente com o negócio da empresa. A gestão de riscos maximiza a segurança e diminui os problemas oriundos de panes, indisponibilidade e perda de informações importantes para o negócio. Dessa maneira, diminui-se a abertura de chamados para a equipe de TI, fazendo com que suas ações sejam voltadas para agregar mais valor a empresa e melhoria de desempenho da equipe.

1.4 GESTÃO DA CONTINUIDADE DOS NEGÓCIOS

 A Gestão da Continuidade dos Negócios ou GCN, segundo a ABNT, é um processo de gestão que identifica as ameaças para uma organização e seus possíveis impactos no negócio caso alguma das ameaças se concretize. A GCN desenvolve uma resiliência na organização para que ela seja capaz de responder às ameaças e reestabelecer rapidamente os serviços afetados.

 A maior parte das organizações começaram a compreender a importância da GCN depois dos ataques terroristas ocorrido em 11 de Setembro ao *World Trade Center* em Nova Iorque, onde muitas organizações deixaram de existir por não terem uma GCN implantada (FONTES, 2008).

 Os incidentes podem ser dos mais variados tipos, mas resultarão em três cenários, são eles: indisponibilidade de acesso físico ao local de trabalho (ex: incêndio, desabamento, enchentes), indisponibilidade de pessoas chaves (ex: afastamento em massa ou por doença) e a indisponibilidade dos recursos de TI (ex: queda do link de internet, dano no datacenter).

 A gestão da continuidade do negócio orienta a definição de medidas para a prevenção da interrupção dos negócios da empresa, não permitindo que haja prejuízos com a paralização dos serviços.

1.5 FERRAMENTAS DE MONITORAMENTO – O ZABBIX

1.5.1 Introdução ao Zabbix

O Zabbix foi projetado e idealizado pelo russo Alexei Vladishev, em 1998, a partir de uma necessidade de monitorar a infraestrutura de um banco ao qual ele trabalhava na Letônia. Atualmente é mantido pela Zabbix SIA Company. O Zabbix é um software de monitoramento de rede open source para empresas, com ele é possível monitorar vários parâmetros de todos os dispositivos de uma rede de computadores. Com o Zabbix é possível também usar mecanismos de notificações seja por e-mail, SMS e mensagem pelo Telegram a partir de qualquer evento nos itens monitorados permitindo assim uma ação rápida a qualquer problema ocorrido na infraestrutura monitorada (ZABBIX, 2018).

Este software oferece também suporte à relatórios e visualização de dados. Com base nos dados armazenados, toda a manutenção, configuração e monitoramento do Zabbix são acessadas por uma interface Web simples e intuitiva. Suporta o monitoramento por vários protocolos como por exemplo SNMP v1 v2 v3 entre outros. O Zabbix configurado corretamente pode desempenhar um papel muito importante no monitoramento da infraestrutura de TI, tanto para pequenas empresas como para grandes organizações (ZABBIX, 2018).

O Zabbix é gratuito e distribuído na licença GPL v2 (*General Public License*), seu código-fonte é distribuído gratuitamente e está disponível para a comunidade em geral. Apesar de ser gratuito, o suporte comercial é dado pela Zabbix INC.

Figura 1: Visão de Geral do Zabbix



Fonte: site oficial do Zabbix (2018)

1.5.2 Características do Zabbix

Abaixo estão listadas as características da ferramenta segundo o site oficial:

* Possui suporte a maioria dos sistemas operacionais: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, NetBSD, Mac OS X, Windows, entre outros;
* Suporte a vários SGBD (*Sistemas Gerenciadores de Banco de Dados*), para a coleta e armazenamento dos dados coletados na infraestrutura de rede monitorada: PostgreSQL, SQLite, MySQL/MariaDB, Oracle e IBM DB2;
* Monitora serviços simples (http, pop3, imap, ssh) sem o uso de agentes;
* Suporte nativo ao protocolo SNMP;
* Interface de gerenciamento Web, de fácil utilização;
* Geração de gráficos em tempo real;
* Fácil instalação e customização;
* Agentes disponíveis para diversas plataformas: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, SCO-OpenServer, Mac OS X, Windows 2000/XP/2003/Vista;
* Agentes para plataformas 32 bits e 64 bits;
* Integração com os Contadores de Performance do Windows;
* Software open source distribuído pela Licença GPL v2;
* Envio de alertas para: e-mail, Jabber, SMS;
* Scripts personalizados;
* Monitoramento de aplicações Java;
* Monitoramento de aplicações Web;
* Monitoramento de ambientes virtualizados;
* Auditoria de sistemas;
* Autodescoberta de dispositivos na rede.

1.5.3 Componentes do Zabbix

Segundo Horst, Pires e Déo (2015) o Zabbix possui 5 componentes principais que são eles: o Zabbix Server (Servidor Zabbix), o Zabbix Proxy (Proxy Zabbix), o Zabbix Agent (Agente Zabbix), a Interface Web e o Banco de Dados.

* Zabbix Server ou Servidor Zabbix - É o componente central da solução e, em ambientes centralizados, os agentes enviam os dados coletados (sobre integridade, disponibilidade e estatísticos) para ele. Em ambientes descentralizados o envio dos dados é feito para um componente intermediário: o proxy.

* Zabbix Proxy ou Proxy Zabbix - Pode coletar dados de desempenho e disponibilidade em nome do Servidor Zabbix. Este é um componente opcional na implantação do Zabbix, no entanto, pode ser muito benéfico para seu ambiente distribuir a carga de coletas entre o Servidor Zabbix e um ou mais proxies.

* Zabbix Agent ou Agente Zabbix - É instalado nos servidores alvos da monitoração e pode monitorar ativamente os recursos e aplicações locais, enviando os dados obtidos para o Servidor ou Proxy Zabbix.

* Interface Web - Provê acesso rápido, a partir de qualquer dispositivo. Normalmente esta interface é parte da mesma máquina do Servidor Zabbix, apesar de ser possível sua instalação em outro servidor.
* Banco de Dados - Guarda todas as informações de configuração, os dados recebidos pelo Zabbix são armazenados nele e gerenciados por um sistema gerenciador de banco de dados (SGBD).

Figura 2: Arquitetura do Zabbix



Fonte/: Zabbix, Zabbix Arquitetura. Acesso em Abril, 2018.

Dessa maneira, com a implantação dessa ferramenta, a equipe de TI estará sempre um passo à frente no que diz respeito aos possíveis problemas que possam vir a acontecer, e assim, poderão tomar as providências necessárias para evitar problemas futuros, ou agir mais rapidamente para que os serviços da empresa voltem a funcionar no seu estado normal.

**4 CONSIDERAÇÕES FINAIS**

 O presente trabalho serviu como fonte de ampliação do conhecimento a respeito da importância do gerenciamento dos serviços de TI para manter uma boa infraestrutura.

 Ter informações corretas e sempre disponíveis em tempo real para que o responsável da TI possa tomar decisões mais assertivas e em tempo mais hábil, minimiza assim a indisponibilidade dos recursos para o usuário final e gera menos impacto para o negócio da empresa.

 Para o correto funcionamento de qualquer infraestrutura de TI é necessário o seu gerenciamento através de ferramentas para verificação de erros em aplicações, falhas nos equipamentos e status dos serviços. A solução proposta neste trabalho foi a utilização da ferramenta Zabbix, que foi escolhida por ser open source e regida sob a licença GPL v2, que para a empresa representa um custo zero caso queira implantar o plano elaborado neste trabalho, tornando-se assim um fator importantíssimo para redução de custos.

**5 REFERÊNCIAS**

COELHO, Flávia Estélia Silva. **Gestão da segurança da informação: NBR 27001 e NBR 27002** / Flávia Estélia Silva Coelho, Luiz Geraldo Segadas de Araújo, Edson Kowask Bezerra. Rio de Janeiro: RNP/ESR, 2014.

GOMES, F. **Plano de Gerenciamento de Riscos do Projeto.** Disponível em: < https://msofficeproject.wordpress.com/2008/09/01/plano-de-gerenciamento-de-riscos-do-projeto/>. 2008. Acesso em: 05/03/2018.

JOÃO, B.N. **Sistemas de Informação.** São Paulo: Pearson Education do Brasil, 2012.

PMBOK. **Um Guia do Conhecimento em Gerenciamento de Projetos** (Guia PMBOK) – Quarta Edição. 2010.

FONTES, E. L. G. **Praticando a Segurança da Informação.** Rio de Janeiro: Brasport, 2008.

1. Discente do curso de Sistemas de Informação da Faculdade Paraíso. [↑](#footnote-ref-1)
2. Docente e Coordenador do curso de Sistemas de Informação da Faculdade Paraíso. [↑](#footnote-ref-2)