CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Douglas Favaro Ferreira

ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Um estudo de caso baseado nas melhores práticas da ISO/IEC 27005

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Douglas Favaro Ferreira

ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Um estudo de caso baseado nas melhores práticas da ISO/IEC 27005

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação do Prof. Esp. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação

Americana, SP

2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

F441a

Ferreira, Douglas Favaro

Análise e avaliação de riscos de segurança da informação: um estudo de caso baseado nas melhores práticas da ISO/IEC 27005. / Douglas Favaro Ferreira. – Americana: 2015.

36f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Esp. Edson Roberto Gaseta

1. Segurança em sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Douglas Favaro Ferreira

Douglas Favaro Ferreira

ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Um estudo de caso baseado nas melhores práticas da ISO/IEC 27005

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/Americana, sob orientação do Prof. Esp. Edson Roberto Gaseta.
Área de concentração: Segurança da Informação

Americana, 09 de dezembro de 2015.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
FATEC Americana

Juliane Borsato Beckedorff Pinto (Membro)
Graduada
FATEC Americana

Rodrigo Brito Battilana
Bacharel
FATEC Americana

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer a Deus por iluminar meu caminho em busca do conhecimento.

Ao Prof. Esp. Edson Roberto Gaseta, pela paciência e disposição do seu tempo na orientação do meu trabalho.

A minha família pelo incentivo e por acreditar no meu potencial, especialmente minha Mãe.

DEDICATÓRIA

Esse trabalho é dedicado a todas as pessoas que contribuíram comigo ao longo desses anos na Faculdade de Tecnologia de Americana (FATEC AMERICANA).

RESUMO

O presente trabalho conceitua o processo de análise e avaliação de riscos de segurança da informação, fundamentando a importância de uma gestão de riscos e de continuidade dos serviços de TI. O trabalho também apresenta, de forma metódica e organizada, todo o processo de análise e avaliação de riscos baseado na norma da ABNT NBR ISO/IEC 27005:2011. Para mostrar esse processo, foi realizado um estudo de caso, no ambiente de TI de uma organização, utilizando de ferramentas desenvolvidas com base no processo de análise e avaliação de riscos apresentado, com a finalidade de identificar os riscos que essa organização está suscetível em relação aos processos do seu negócio.

Palavras chaves: Segurança da Informação; Gestão de Risco; ISO 27005.

ABSTRACT

The present text conceptualizes the process of analysis and assessment of information security risks, grounding the importance of risk management and continuity of IT services. Its also introduces, in a methodical and organized way, the whole process of analysis and assessment based on the standard rules of ISO/IEC 27005:2011. To show this process, a case study was conducted in an IT environment of an specific organization, using developed tools based on the process of analysis and assessment presented, in order to identify the risks that the mentioned organization is susceptible in relation to its your business processes.

Keywords: Information Security; Risk Manager; ISO 27005.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

As organizações são totalmente dependentes da tecnologia da informação (TI) para administração e desenvolvimento do seu negócio. A falta de investimento e auditoria nos sistemas de informação das empresas e em toda infraestrutura que comporta o sistema, a fim de identificar e evitar possíveis vulnerabilidades que possam vir a serem exploradas pode causar um alto impacto nos negócios dessas organizações.

O objetivo geral desse trabalho é apresentar como funciona o processo de análise e avaliação de riscos de segurança da informação, capaz de identificar vulnerabilidades com alta capacidade de serem exploradas, que podem causar impacto no negócio e estratégia de uma organização. As ferramentas utilizadas para a classificação e avaliação dos riscos, são baseadas nas melhores práticas da ABNT NBR ISO/IEC 27005:2011 (ABNT, 2011).

O objetivo específico é testar um modelo de análise e avaliação de riscos em uma organização, levantando os principais pontos em que a TI influencia no negócio e mostrando que seus ativos podem impactar negativamente na estratégia da organização, caso algum evento adverso aconteça.

O resultado será apresentado e detalhado, para mostrar a importância do processo de análise e avaliação de risco nesse ambiente e também para posteriormente, comunicar a organização estudada sobre as ameaças que cercam o seu negócio.

O método científico de pesquisa utilizado é baseado na norma da ABNT NBR ISO/IEC 27005:2011, que apresenta um conjunto de ferramentas para serem utilizadas durante o processo de análise e avaliação de riscos. Essas ferramentas foram adaptadas conforme o ambiente estudado, a fim de oferecer resultados mais precisos sobre os ativos analisados.

O trabalho foi estruturado em cinco capítulos, sendo que o primeiro traz conceitos importantes de segurança da informação. O segundo mostra o conceito de gestão de risco e continuidade de serviços de TI, que utiliza do processo de

análise e avaliação de riscos como ferramenta para implementação do processo. O terceiro traz o conceito do processo de análise e avaliação de riscos, de acordo com a norma da ABNT NBR ISO/IEC 27005:2011, onde as etapas são descritas detalhadamente. O quarto capítulo apresenta o estudo de caso, com a aplicação da ferramenta de análise e avaliação no ambiente de uma organização específica. O quinto capítulo conclui o estudo de caso e traz as considerações finais sobre o trabalho.

2. SEGURANÇA DA INFORMAÇÃO

Com a evolução da tecnologia e a informatização das organizações, surgiu a necessidade de proteger as informações armazenadas nos sistemas de informações e o tema segurança da informação começou a fazer parte do cotidiano dos profissionais e departamentos de TI das empresas.

Segundo Lyra (2008, p.4) “Quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações”. É importante destacar esses aspectos que compõem a segurança da informação:

- Confidencialidade: capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo em que impede que outros, não autorizados, a vejam.
- Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.
- Disponibilidade: informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais

Quando algum desses aspectos é violado, ocorre um incidente de segurança. Lyra (2008, p.5), define que “incidente de segurança é a ocorrência de um evento que possa causar interrupções nos processos de negócio em consequência da violação de algum dos aspectos de segurança da informação”.

Um incidente pode ser evitado através de um mapeamento da infraestrutura de TI com a finalidade de identificar as vulnerabilidades presentes no ambiente, para posteriormente, realizar-se uma análise dos riscos presentes nesse ambiente, caso essas vulnerabilidades sejam exploradas por um agente externo ou interno.

3. GESTÃO DE RISCO

Em um estudo recente da empresa IBM, publicado pelo site ComputerWord, são listados alguns desafios enfrentados pelos gestores nas organizações, em relação a segurança da informação. Segundo o estudo:

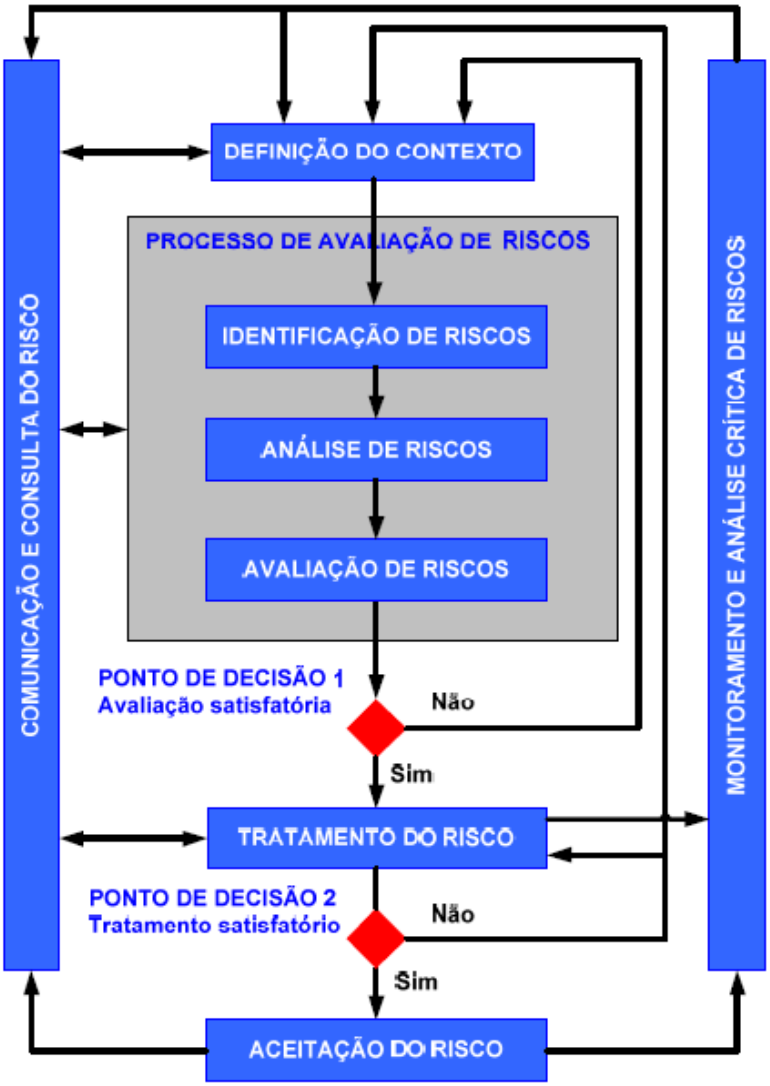
> "O primeiro é focar ações de proteção em temas estratégicos, transformando um programa baseado em compliance em um orientado a gestão de riscos. Outro é sobre comunicar prioridades para gerar sensibilidade e priorizar questões de proteção." (DREHER, 2015).

Esses itens mostram como é importante o TI estar alinhado à estratégia da organização, para identificar e proteger pontos de alta criticidade para o negócio. E para isso, é necessário que a empresa tenha uma gestão de risco no seu ambiente de TI.

O processo de gestão de riscos de segurança da informação, segundo a norma da ABNT NBR ISO/IEC 27005:2011, consiste na "definição de contexto, processo de avaliação de riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica de riscos" (ABNT, 2011).

A Figura 1 mostra cada um desses itens que compõem a gestão de riscos e sua iteração no decorrer do processo.

Figura 1: Processo de Gestão de Riscos



Fonte: ABNT 2011

Os componentes do processo de gestão de riscos são iterativos conforme apresentado na figura 1. A norma da ISO/IEC 27005 explica que “Um enfoque iterativo na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição” (ABNT, 2011). Com o monitoramento e a comunicação de riscos, o tempo despendido no processo é gasto com mais eficiência e eficácia.

Com o contexto definido, o processo de identificação dos riscos é realizado levando em conta os ativo de TI da organização. Após a identificação, o processo de avaliação de riscos é executado e caso ele forneça informações suficientes

para reduzir o risco a um nível aceitável, a tarefa de tratamento de risco é executada e pode ser sucedida. Mas caso o processo de avaliação de riscos não apresente informações suficientes, outra iteração é realizada, revisando o contexto para adquirir mais informações. O tratamento do risco depende do processo de avaliação de riscos, para ter eficácia.

A aceitação do risco depende do processo de tratamento. Caso ele apresente um risco residual que não seja aceitável, é necessária uma nova iteração no processo de avaliação de riscos, até que o risco residual chegue a um nível aceitável.

3.1 Governança de TI

Um dos principais frameworks para implementação de uma Governança de TI é o *COBIT (Control Objectives for Information and related Technology)*. Em sua documentação, é definido que

> A governança garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos. (ISACA, 2012, p.16)

O *COBIT* possui quatro domínios, baseados na metodologia PDCA (Planejar, Executar, Verificar e Monitorar) divididos em 37 processos de práticas de governança e de gestão em TI. Um desses processos é o de gerenciamento de riscos, que identifica possíveis cenários de riscos dentro de uma organização. Segundo o *COBIT,* “um cenário de riscos de TI é uma descrição de um evento relacionado a TI que pode causar um impacto nos negócios, quando e se ele ocorrer.” (ISACA, 2012)

A principal vantagem do processo de gerenciamento de riscos dentro da governança de TI é de que com os cenários de riscos, as pessoas desenvolvem uma variedade de resultados possíveis, pensando de forma mais abrangente e se preparam melhor para a gama de possibilidade que o futuro pode trazer (Fischer, 2011).

3.2 Continuidade dos Serviços de TI

A gestão de riscos é utilizada dentro da *ITIL (Information Technology Infrastructure Library)*. Esse framework é detalhado no livro “Gerenciamento de Serviços de TI na Prática”, do autor Magalhães (2007, p.61), que define:

> A ITIL fornece orientações para a área de TI baseadas nas melhores práticas e em um ambiente de qualidade, visando à melhoria contínua, envolvendo pessoas, processos e tecnologia, objetivando o gerenciamento da área de TI como um negócio dentro do negócio da organização”.

Dentre os vários processos dessa ferramenta de boas práticas a serem implementadas como um modelo de gerenciamento de TI de qualidade, o processo de Gerenciamento de Continuidade dos Serviços expõe a necessidade e importância de ter uma gestão de riscos madura nas organizações.

> O Gerenciamento de Continuidade dos Serviços de TI tem por escopo dar suporte à continuidade dos serviços de TI que suportam os processos de negócio da organização, garantindo, dessa forma, que tais serviços possam ser recuperados no menor intervalo de tempo possível [...] (MAGALHÃES, 2007, p.411).

O processo de análise e avaliação de riscos é o ponto inicial para implementação de uma cultura de gestão de riscos nas organizações para apoiar na Continuidade dos Serviços de TI, informando a organização sobre ameaças que podem impactar nos serviços de TI e no negócio, apontando as consequências para o negócio caso algum serviço venha ser comprometido.

4. ANÁLISE E AVALIAÇÃO DE RISCO

4.1 Definição de Contexto

A norma ISO/IEC 27005, estabelece que definição de contexto são “todas as informações sobre a organização relevantes para a definição do contexto da gestão de riscos de segurança da informação” (ABNT, 2011).

Levantada as informações da organização, os critérios básicos de avaliação, impacto e aceitação, serão definidos de acordo com o que foi estabelecido no escopo da definição de contexto.

4.1.1 Critérios de Avaliação

Os critérios de avaliação de risco são necessários para avaliar os riscos de uma organização. Para compor esses critérios, itens estratégicos do negócio são utilizados pela ISO/IEC 27005, como criticidade dos ativos, valor estratégico para o negócio, importância no ponto de vista operacional e expectativa e consequência para o valor do negócio, imagem e reputação da organização.

4.1.2 Critérios de Impacto

Os critérios de impacto são desenvolvidos em função dos danos ou custos à organização, causados por um risco de segurança da informação. Esses critérios são desenvolvidos considerando, por exemplo, dano a reputação, ocorrência de violação de SI, operações do negócio comprometidas, dentre outros sugeridos pela ISO/IEC 27005.

4.1.3 Critérios para aceitação do risco

Os critérios para aceitação de riscos, segundo a norma da ISO/IEC 27005, são desenvolvidos e especificados em acordo com as políticas, metas e objetivos da organização. Para que os critérios de aceitação do risco sejam estabelecidos, a norma sugere que sejam considerados, critérios do negócio, operações, tecnologia, finanças e fatores sociais e humanitários.

4.2 Escopo e Limites

O escopo da gestão de riscos de segurança da informação é definido para assegurar que todos os ativos relevantes sejam considerados no processo de avaliação de riscos. Com isso, é possível determinar o ambiente em que a organização opera e relevância dele para o processo de gestão de riscos de segurança da informação.

Para definir o escopo, convém que a organização considere itens estratégicos como objetivos, políticas e processos; funções e estruturas da organização; ativos de informação e abordagem da organização à gestão de risco.

4.3 Identificação de Riscos

4.3.1 Identificação dos Ativos

A norma da ISO/IEC 27005 define que “um ativo é algo que tem valor para a organização e que, portanto, requer proteção” (ABNT, 2011). A identificação dos ativos deve ser realizada detalhadamente, para que forneça informações suficientes para o processo de análise e avaliação de riscos.

É importante salientar, que os ativos que compõem um sistema de informação, compreende mais do que hardware e software; recursos humanos, rede e infraestrutura física, são outros ativos que suportam os principais, que são processos e atividades do negócio e informação.

4.3.2 Identificação das Ameaças

Uma ameaça tem o potencial de comprometer um ativo. A ISO/IEC 27005, diz que “as ameaça podem ser de origem natural ou humana e podem ser acidentais ou intencionais” (ABNT, 2011). Portanto, é importante que todas as ameaças sejam identificadas, evitando o comprometimento de informações, processos e sistemas de um ativo.

Para identificação da ameaça e análise da probabilidade, as informações são levantas por especialistas de segurança e pessoas envolvidas com a organização.

4.3.3 Identificação das Vulnerabilidades

As vulnerabilidades podem ser identificadas nos recursos humanos, ambiente físico, processos e procedimentos, hardware e software de equipamentos e em diversas outras áreas da organização.

Uma vulnerabilidade torna-se um risco, quando existe uma ameaça para explorá-la. Por isso, no processo de identificação, é importante destacar as vulnerabilidades associadas a ameaças e as vulnerabilidades associadas a nenhuma ameaça para análise.

4.3.4 Identificação das Consequências

A ISO/IEC 27005 define que uma “consequência pode ser a perda da eficácia, reputação afetada, condições adversas de operação e prejuízo” (ABNT, 2011). A identificação necessária para evitar essas consequências em um cenário de incidente (quando uma ameaça explorar uma determinada vulnerabilidade com êxito).

Após a identificação, uma lista é formada com os cenários de incidentes, classificados de acordo com os critérios de impacto, descritos previamente na definição de contexto.

4.4 Análise de Riscos

4.4.1 Metodologia de análise de risco

A norma da ISO/IEC 27005, diz que “a análise de risco pode ser empreendida com diferentes graus de detalhamento” (ABNT, 2011). Por isso, existem duas metodologias utilizadas para análise de riscos: a qualitativa e a quantitativa.

A análise qualitativa utiliza uma escala descritiva, com atributos que classificam a magnitude da consequência e a probabilidade dela ocorrer. A análise quantitativa utiliza uma escala de valores numéricos, usando dados históricos de diversas fontes, para classificar o nível da magnitude e de probabilidade do risco.

A escolha da metodologia irá variar de acordo com o risco e do propósito de um projeto análise e avaliação que está sendo implementada.

4.4.2 Avaliação das Consequências

O impacto sobre o negócio causado por incidentes que violem algum aspecto da segurança da informação é uma consequência que deve ser avaliada. Uma consequência tem um valor de impacto, que dever ser avaliada de acordo com sua criticidade. O valor é determinado de duas maneiras: através do valor de reposição do ativo; e através da perda ou comprometimento do ativo, que gera consequências adversas a organização, como indisponibilidades de sistemas e suas informações.

Portanto, as consequências podem ser expressas em função dos critérios monetários, técnicos ou humanos, que geram impactos ou algum outro comprometimento do negócio na organização.

4.4.3 Avaliação da Probabilidade de Incidentes

A avaliação da probabilidade de incidentes é realizada com base nos cenários de incidentes identificados, com a finalidade de identificar os possíveis impactos causados no ambiente estudado.

A norma da ISO 27005, diz que “convém levar em conta a frequência da ocorrência das ameaças e a facilidade com que as vulnerabilidades podem ser exploradas, levando em conta ameaças acidentais, intencionais, vulnerabilidade e histórico de ocorrência da ameaça” (ABNT, 2011).

4.4.4 Determinação do Nível do Risco

Os níveis de risco são estimados de acordo com os cenários dos incidentes identificados previamente. Segundo a norma ISO/IEC 27005, “o risco estimado é uma combinação da probabilidade de um cenário de incidente e suas consequências” (ABNT, 2011). Essa análise pode levar em conta o custo-benefício, as preocupações das partes interessadas e outras variáveis acordadas durante o processo.

4.5 Avaliação de Riscos

Os critérios de avaliação de risco serão comparados com os critérios de nível de riscos, que devem ser consistentes com o contexto da organização. A norma da ISO/IEC 27005, diz que “convém que os critérios de avaliação, sejam consistentes com o contexto definido, relativo à segurança da informação” (ABNT, 2011).

Itens como propriedades da segurança da informação, devem ser levados em conta, para avaliar um risco e determinar o seu nível de relevância para a organização. A atividade suportada por determinado ativo, também são levados em conta no processo de avaliação e classificação da relevância.

5. ESTUDO DE CASO

5.1 Definição de Contexto

A empresa estudada é líder nacional no segmento de bebidas não alcoólicas e atua na fabricação de sucos, chás, isotônicos, energéticos e outras bebidas prontas para beber. Atualmente conta com unidades fabris nos estados de São Paulo, Espírito Santo, Rio de Janeiro e Paraná; possuindo mais de 2600 funcionários.

Apesar dos investimentos na área de tecnologia da informação, o departamento ainda não é visto como uma parte vital, para estratégica do negócio, não tendo um modelo de governança adequado para prover auditorias na sua infraestrutura, podendo comprometer a saúde do negócio.

5.1.1 Critério de Impacto

Para esse estudo, os critérios de impacto foram definidos de acordo com o impacto no negócio e a violação de algum atributo de SI. Os níveis foram definidos em alto, médio e baixo, conforme exemplificado na Tabela 1. As ameaças que atenderem esses dois critérios irão continuar no processo de análise e avaliação de riscos.

Tabela 1: Critérios de Impacto

	NIVEL DE IMPACTO		
CRITÉRIO	ALTA	MÉDIO	BAIXA
IMPACTO NO NEGÓCIO	Paralisação de processos críticos da empresa.	Alguns processos podem ser afetados. Perda de eficiência em alguns serviços do negócio.	Efeitos mínimos para o negócio.

Fonte: Autor

5.1.2 Critério de Avaliação

Serão considerados e classificados como riscos graves e com necessidade de tratamento imediato, riscos que impactem diretamente em algum processo do negócio, que atinjam algum atributo da segurança da informação e/ou que causem danos à imagem e reputação da organização.

Esses riscos serão classificados de acordo com o Nível de Risco (NR), resultado do Nível de Impacto (NI) e o Nível de Probabilidade (NP) e os critérios serão os responsáveis pela priorização do risco em casos em que os NRs sejam iguais.

5.1.3 Critério de Aceitação do Risco

Os critérios foram definidos de acordo com o NR das ameaças. A aceitabilidade foi definida de acordo com os objetivos do negócio, assim, riscos com maior impacto em algum processo do negócio, foram classificados como inaceitáveis e requerem tratamento imediato; os riscos que não impactam no negócio, podem ser aceitos e seu tratamento pode ser discutido em segundo plano dentro da organização. A Tabela 2 foi utilizada para sistematização do processo e fácil identificação de como o risco deve ser priorizada dentro da organização.

Tabela 2: Critério para Aceitação do Risco

NIVEL DE RISCO (1 - 9)	DESCRIÇÃO	ACEITABILIDADE
ALTO (6 - 9)	Os objetivos do negócio são impactados. Algum serviço necessário para o Negócio é paralisado.	Risco inaceitável. Requer ação imediata para tratamento.
MÉDIO (3 - 5)	Alguns objetivos do negócio são impactados. Alguns processos são afetados.	Risco inaceitável. Requer ação para tratamento.
BAIXO (1 - 2)	Efeitos secundários, que não causam impacto no negócio.	Risco Aceitável, nenhuma ação imediata é requerida.

Fonte: Autor

5.2 Identificação dos Riscos

5.2.1 Identificação dos Ativos

Os ativos foram identificados levando em consideração sua relevância para o negócio e para segurança das informações relacionadas à organização. Foi detalhada a função de cada ativo e a interação dele com o negócio. A Tabela 3 traz todas essas informações que foram levantadas.

Tabela 3: Identificação dos Ativos

IDENTIFICAÇÃO DOS ATIVOS	
Ativo	Função
Computador Supervisório Produção	Esse equipamento é responsável por controlar e monitorar todo o processo de preparação do produto produzido na organização, até o ponto de embalo.
Computador Supervisório E.T.A (Estação de Tratamento de Água)	Equipamento responsável por monitorar e controlar todo o fluxo de água dos poços, que são enviados para a caixa d'água e em seguida, para a produção.
CPD (Infraestrutura Geral)	Local onde estão centralizados os serviços de rede, internet, arquivo e outros serviços servidor-cliente
Servidor ProdWin (Sistema de controle da produção)	Ativo responsável por receber todas as informações da linha de produção (Tempo de parada, tempo de execução, motivo de parada, dentre outros)
Link de Dados	Responsável pela comunicação da filial estudada, com as outras filiais, matriz e locais externos
Servidor de Arquivos	Local onde estão armazenados os arquivos dos usuários e departamentos.
Switchs (Fora do CPD)	Switchs secundários, que recebem o fluxo de informação dos switchs do backbone
Servidor Supervisório Produção	Equipamento que recebe os dados do processo de produção do negócio e envia para os computadores que realizam o monitoramento e controle

Fonte: Autor

5.2.2 Identificação das Ameaças

As ameaças foram identificadas, baseadas na lista de ativos levantados. Foram levadas em conta ameaças conhecidas do dia-a-dia e ameaças que já ocorreram na organização estudada. A Tabela 4 apresenta essas ameaças, identificadas com o seu tipo e a fonte (acidental, intencional ou natural).

Tabela 4: Identificação das Ameaças

IDENTIFICAÇÃO DAS AMEAÇAS		
Ameaça	Tipo	Fonte
Danificação do equipamento	Dano Físico	A - I - N
Queda do Link de Dados	Paralisação de Serviço	A - I
Acesso Indevido	Comprometimento da Informação	I
Indisponibilidade de Dados	Comprometimento da Informação	A - I

Fonte: Autor

5.2.3 Identificação das Vulnerabilidades

As vulnerabilidades foram levantas com base nas ameaças relatadas. As informações foram levantas através de uma análise e inspeção dos ativos identificados. A Tabela 5 apresenta essas vulnerabilidades relacionadas com os ativos.

Tabela 5: Identificação das Vulnerabilidades

IDENTIFICAÇÃO DAS VULNERABILIDADES	
Vulnerabilidade	Ativo Relacionado
Indisponibilidade de um equipamento backup em caso de parada do atual	Computador Supervisório Produção Computador Supervisório E.T.A (Estação de Tratamento de Água)
Falta de uma rotina de manutenção e/ou substituição periódica	Computador Supervisório Produção Computador Supervisório E.T.A (Estação de Tratamento de Água)
Falta de rotina de backup do servidor	Servidor ProdWin (Sistema de controle da produção)
Inexistência de políticas de auditoria e controle de permissões dos arquivos.	Servidor de Arquivos
Falta de um No-Break para estabilização da rede elétrica.	Switch (fora do CPD) e CPD
Link principal e de contingência chegam na mesma infraestrutura.	Link de Dados

Fonte: Autor

5.2.4 Identificação das Consequências

As consequências levantadas mostram a perda que o negócio sofre caso uma ameaça seja concretizada. Os cenários relatam incidentes e o prejuízo para o negócio em termos de segurança da informação e indisponibilidade de processos que o compõem. A Tabela 6 mostra todos os cenários identificados.

Tabela 6: Identificação das Consequências

IDENTIFICAÇÃO DAS CONSEQUÊNCIAS	
Consequência	Ativo
Indisponibilidade do monitoramento e controle dos poços e caixa d'agua (Sistema automatizado). Interrupção de processo necessário para o funcionamento do negócio.	Computador Supervisório E.T.A (Estação de Tratamento de Água)
Indisponibilidade de informações consideradas críticas para controle da qualidade do produto do negócio. Interrupção de processo necessário para o funcionamento do negócio.	Computadores Supervisório Produção
Perda da eficiência do negócio. Indisponibilidade de sistemas, telefonia, rede, etc. (Processos secundários do negócio)	CPD (Infraestrutura Geral)
Perda da eficiência do negócio. Indisponibilidade de sistemas, telefonia, rede, etc.	Link de Dados
Perda da confidencialidade e integridade dos dados. Possível indisponibilidades de arquivos necessários para o processo.	Servidor de Arquivos
Perda da integridade dos dados. Perda de eficiência do negócio (Dados sobre o negócio são afetados).	Servidor ProdWin (Sistema de controle da produção)
Perda da disponibilidade dos dados. Indisponibilidade de sistemas, telefonia, rede, etc. em alguns pontos do site.	Switchs (Fora do CPD)

Fonte: Autor

5.3 Análise de Riscos

5.3.1 Metodologia da Análise

Para o processo de análise do risco, a metodologia qualitativa foi utilizada. Os valores de 1 a 3 (1 para baixo, 2 para médio e 3 para alto) foram utilizados para pontuar o Nível de Impacto e o Nível de Probabilidade, que combinados, geraram o Nível de Risco (NR) da ameaça, que varia de 1 à 9.

5.3.2 Avaliação de Probabilidade

Essa avaliação irá pontuar a probabilidade de um incidente acontecer no ambiente identificado. Foi considerado na avaliação, o nível de recorrência da ameaça analisada e qual o nível de facilidade de exploração da vulnerabilidade do ativo. A tabela 7 representa essa avaliação e os valores foram pontuados no processo de determinação do risco.

Tabela 7: Avaliação da Probabilidade

Critério	Alto	Médio	Baixo
Probabilidade da Ameaça	Ameaças comuns que ocorrem no dia-a-dia de uma empresa.	Ameaças não-comuns, mas que ocorrem com uma freqüência variável	Ameaças não-comuns, que dependem da facilidade de exploração.

Fonte: Autor

5.3.3 Determinação do Nível de Risco

Nesse processo, o nível de risco (NR) das ameaças será estimado a partir da combinação do nível de impacto (NI) e o nível de probabilidade (NP) da ameaça. A Tabela 8 será utilizada como referência para identificação do NR.

Tabela 8: Matriz de Risco

	Nível de Probabilidade (NP)	Baixa (1)	Média (2)	Alta (3)
Nível de Impacto (NI)	Alta (3)	3	6	9
	Média (2)	2	4	6
	Baixa (1)	1	2	3

Nível de Risco Alto | Nível de Risco Médio | Nível de Risco Baixo

Fonte: Autor

Com o nível de risco identificado dos cenários dos incidentes levantados, o processo de análise de risco é concluído. Todas as etapas da análise de risco estão listadas em uma única tabela (tabela 8) e podemos ver o resultado final de processo, com os níveis de impacto, probabilidade e consequentemente o de riscos estimados.

Tabela 8 – Análise de Riscos

ANÁLISE DE RISCOS							
Identificação de Riscos					Estimativa de Riscos		
Nº	**Ativo**	**Ameaça**	**Vulnerabilidade**	**Consequência**	**NI**	**NP**	**NR**
1	Computador Supervisório E.T.A (Estação de Tratamento de Água)	Danificação de equipamento	Indisponibilidade de um equipamento backup em caso de parada do atual	Indisponibilidade do monitoramento e controle dos poços e caixa d'água (Sistema automatizado). Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
2	Computador Supervisório E.T.A (Estação de Tratamento de Água)	Danificação de equipamento	Falta de uma rotina de manutenção e/ou substituição periódica	Indisponibilidade do monitoramento e controle dos poços e caixa d'agua (Sistema automatizado). Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
3	Computadores Supervisório Produção	Danificação de equipamento	Falta de uma rotina de manutenção e/ou substituição periódica	Indisponibilidade de informações consideradas críticas para controle da qualidade do produto do negócio. Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
4	Computadores Supervisório Produção	Danificação de equipamento	Indisponibilidade de um equipamento backup em caso de parada do atual	Indisponibilidade de informações consideradas críticas para controle da qualidade do produto do negócio. Interrupção de processo necessário para o funcionamento do negócio.	3	2	6
5	CPD (Infraestrutura Geral)	Danificação de equipamento	Falta de No-Break para estabilização da rede elétrica	Perda da eficiência do negócio. Indisponibilidade de sistemas, telefonia, rede, etc (Processos secundários do negócio)	3	1	3

ANÁLISE DE RISCOS							
Identificação de Riscos					Estimativa de Riscos		
Nº	**Ativo**	**Ameaça**	**Vulnerabilidade**	**Consequência**	**NI**	**NP**	**NR**
6	Link de Dados	Queda do Link de Dados	Rompimento da fibra óptica. Link principal e de contingência chegam na mesma infraestrutura.	Perda da eficiência do negócio. Indisponibilidade de sistemas, telefonia, rede, etc	2	1	2
7	Servidor de Arquivos	Acesso Indevido	Inexistência de políticas de auditoria e controle de permissões dos arquivos.	Perda da confidencialidade e integridade dos dados. Possível indisponibilidades de arquivos necessários para o processo.	2	2	4
8	Servidor ProdWin (Sistema de controle da produção)	Danificação do equipamento	Indisponibilidade de um equipamento backup em caso de parada do atual	Perda da integridade dos dados. Perda de eficiência do negócio (Processo necessário para o funcionamento do negócio).	3	2	6
9	Servidor ProdWin (Sistema de controle da produção)	Indisponibilidade de Dados	Falta de rotina de backup do servidor	Perda da integridade dos dados. Perda de eficiência do negócio (Dados sobre o negócio são afetados).	3	2	6
10	Switchs (Fora do CPD)	Danificação do equipamento	Falta de equipamento para estabilização da rede elétrica	Perda da disponibilidade dos dados. Indisponibilidade de sistemas, telefonia, rede, etc em alguns pontos do site.	2	1	2

Fonte: Autor

5.4 Avaliação de Riscos

No processo de avaliação de riscos, as ameaças analisadas anteriormente foram classificadas e priorizadas de acordo com o seu nível de risco e outras informações, como impacto no negócio e violação de algum atributo de segurança da informação. A tabela 10, lista esses riscos ordenados por prioridade de tratamento, assim apresentando os principais riscos a serem mitigados de acordo com o escopo considerado.

Tabela 10: Avaliação dos riscos

Nº	Cenário	NR	Algum processo estratégico do negócio é atingido?	Algum ativo crítico é atingido?	Quais atributos de Segurança da Informação são atingidos?	Priorização dos ricos
1	Indisponibilidade de um equipamento backup em caso de parada do atual	6	Sim	Sim	I/D	1
2	Destruição do equipamento devido à falta de uma rotina de manutenção e/ou substituição periódica	6	Sim	Sim	I/D	2
3	Destruição do equipamento devido à falta de uma rotina de manutenção e/ou substituição periódica	6	Sim	Sim	I/D	3
4	Indisponibilidade de um equipamento backup em caso de parada do atual	6	Sim	Sim	I/D	4
8	Indisponibilidade de um equipamento backup em caso de parada do atual	6	Sim	Sim	I/D	5
9	Indisponibilidades dos dados por falta de uma rotina de backup do servidor	6	Sim	Sim	I/D	6
7	Perda de dados devido a inexistência de políticas de auditoria e controle de permissões dos arquivos.	4	Não	Sim	I/D/C	7
5	Danificação dos equipamentos devido à falta de No-break para estabilização da rede elétrica	3	Não	Sim	C	8
10	Danificação dos equipamentos devido à falta de No-break para estabilização da rede elétrica	2	Não	Não	I/D	9
6	Indisponibilidade do link de dados devido a rompimento de fibra. Link principal e de contingencia chegam na mesma infraestrutura.	2	Não	Não	D	10

Fonte: Autor

6. CONCLUSÃO

Com o processo de análise a avaliação de riscos concluídos, as informações serão apresentadas para a organização estudada, a fim de orientar o departamento de tecnologia da informação da empresa no processo de mitigação dos riscos presentes no ambiente de TI. Com isso, espera-se que a organização atinja um nível de maturidade para visualizar a TI como parte integrante e fundamental para o seu negócio e que expanda esse processo de análise e avaliação de riscos para as suas outras filiais.

6.1 Considerações Finais

A ferramenta proposta para realização do processo de análise e avaliação de riscos é de baixo custo e fácil compreensão, oferecendo uma análise primária, mas eficiente, dos riscos presentes no ambiente de tecnologia da informação de uma organização, que podem impactar processos essências para o negócio e do ambiente de TI.

Isso apenas mostra como problemas enfrentados pelas organizações no dia-a-dia e que trazem grandes problemas, poderiam ser identificados e mitigados antecipadamente, apenas com um processo de análise e avaliação de fácil implementação, que toda empresa poderia ter.

Esse trabalho tratou o processo de análise e avaliação de risco com um enfoque de alto nível. Para trabalhos futuros, o processo de gestão de risco será tratado por completo, a fim de desenvolver um processo de continuidade de serviços de TI, dentro da organização estudada, expandindo para todas as suas filiais, garantindo que os ativos envolvidos em processos do negócio, estejam com suas vulnerabilidades mapeadas e em caso de confirmação de um risco, um plano de ação para tratamento e continuidade do serviço esteja pronto, minimizando os impactos gerados no negócio.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS E TÉCNICAS – ABNT. **NBR ISO/IEC 27005**: Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2011. p. 87.

DREHER, Felipe. **Há um verdadeiro caos de governança de segurança da informação**, 2015. Disponível em: <http://computerworld.com.br/ha-um-verdadeiro-caos-de-governanca-na-seguranca-da-informacao-afirma-ibm>. Acesso em: 13 de Nov. 2015.

FISCHER, Urs. **Análise de cenários de TI em gestão de riscos corporativos**. ISACA Journal, 2011. Disponível em: <http://www.isaca.org/Journal/Documents/jpdf11v2-it-scenario-analysis-pt.pdf>. Acesso em: 10 de Dez. 2015

ISACA. **COBIT 5: Modelo corporativo para governança e gestão de TI**. Information Systems Audit and Control Association, 2012. p. 16.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas da Informação**. Rio de Janeiro: Ciência Moderna, 2008. p. 263.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de Serviços de TI na Prática:** Uma Abordagem com Base na ITIL. São Paulo: Novatec, 2007. p. 672.