Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

JONES JOSÉ CORREIA JÚNIOR

MODELO PRÁTICO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA ORGANIZAÇÕES

Brasília
2014

JONES JOSÉ CORREIA JÚNIOR

MODELO PRÁTICO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA ORGANIZAÇÕES

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. MSc. Gilberto Oliveira Netto

Brasília
2014

JONES JOSÉ CORREIA JÚNIOR

MODELO PRÁTICO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA ORGANIZAÇÕES

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. MSc. Gilberto Oliveira Netto

Brasília, 15 de dezembro de 2014.

Banca Examinadora

_____

Prof. Me. Francisco Javier de Obaldia Diaz

_____

Prof. Dr. José Eduardo Brandão

À minha família que, entre altos e baixos, sempre esteve ao meu lado.

RESUMO

Essa pesquisa analisa as recomendações da norma técnica ISO 27005:2011, que trata da gestão de riscos de segurança da informação, e apresenta um modelo prático de gestão de riscos a ser implementado de forma fácil por organizações que desejam assegurar a disponibilidade, integridade e confidencialidade de suas informações. A gestão de riscos é um processo holístico que engloba todas as atividades, processos e recursos que tenham participação na segurança das informações da empresa. Envolve um estudo aprofundado de todos os ativos e informações que se deseja proteger; identificação de todos os riscos que possam comprometer a segurança desses ativos e informações; implementação de soluções de segurança de forma a mitigar os riscos identificados a níveis aceitáveis pelos gestores; e monitoramento contínuo dos riscos, considerando o impacto que esses riscos podem trazer para a segurança da informação se algum evento adverso ocorrer. O modelo proposto foi aplicado, para fins de validação e demonstração, em uma instituição de ensino fictícia.

Palavras-chave: Riscos. Gestão de Riscos. Segurança da Informação.

ABSTRACT

This research analyzes the technical standard ISO 27005:2011 recommendations, which addresses the information security risks management, and presents a practical model of risk management to be implemented easily by organizations that want to ensure the availability, integrity and confidentiality of their information. Risk management is a holistic process that encompasses all activities, processes and resources that take part in the security of company information. It involves a deep study of all assets and information to be protected; identification of all risks that may compromise the security of these assets and information; implementation of security solutions to reduce the identified risks to acceptable levels by managers; and continuous monitoring of risks, considering the impact that these risks can bring to information security if an adverse event occurs. The proposed model was applied in a fictional educational institution, in order to validate as well as demonstrate it.

Key words: Risks. Risk Management. Information Security.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

A informação tornou-se um ativo de fundamental importância para as empresas. Para manterem-se competitivas, as empresas investem cada vez mais em ferramentas para obter, gerenciar e compartilhar informações sobre tudo o que afete o negócio da empresa, de forma a subsidiar o processo de tomada de decisões.

Nos últimos anos, a evolução tecnológica tornou ainda mais crítico o papel da informação no alcance da missão e dos objetivos das empresas. Como descreve Marcos Sêmola (2003. p. 11), décadas atrás as informações eram tratadas de forma centralizada e pouco automatizadas. Ao longo do tempo, o compartilhamento de informações passou a ser considerado necessário para que as empresas acelerassem o desenvolvimento dos negócios. As tecnologias da Informação (TIs) permitiram que as empresas agregassem maior valor aos processos, produtos e serviços, o que conferiu maior dinamismo ao ambiente corporativo. Nesse sentido, percebe-se uma dependência cada vez maior das empresas em relação às tecnologias da informação.

Paralelamente à evolução de tecnologias aplicadas aos negócios, evoluíram também às ameaças às informações das empresas. Protegê-las significa garantir a continuidade e prosperidade do negócio. Trata-se portanto da Segurança da Informação, área do conhecimento que se refere ao processo de proteger informações das ameaças à sua integridade, disponibilidade e confidencialidade. Esses três últimos conceitos são comumente referidos na literatura científica como objetivos ou requisitos fundamentais da segurança da informação.

A confidencialidade garante que informações não sejam reveladas a indivíduos não autorizados. A integridade assegura que dados e sistemas de informação não sejam modificados ou destruídos de forma não autorizada. Por fim, a disponibilidade garante o acesso e uso das informações e ativos associados por usuários legítimos e em tempo adequado (STALLINGS; BROWN, 2014, p.8).

Como forma de se protegerem contra as ameaças às informações, algumas empresas passaram a considerar os riscos à segurança da informação nos seus processos de gestão. A gestão de riscos de segurança da informação envolve

a identificação dos ativos que necessitam de proteção, levantamento e avaliação dos riscos para cada ativo e, implementação de controles gerenciais, operacionais e técnicos para reduzir os riscos a níveis aceitáveis.

A gestão de riscos, contudo, não foi criada a partir da necessidade de se proteger as informações contra as ameaças à segurança da informação. Risco, segundo o Guia ISO 73 que trata do vocabulário de gestão de riscos, é o efeito da incerteza nos objetivos. Ora, o ato de reduzir as incertezas e controlar as variáveis a fim de garantir o alcance dos objetivos há muito já é praticado pelo homem. O que se observou no século XX, foi a incorporação e aprimoramento, por parte das empresas, de técnicas para lidar com riscos com o objetivo de se tornarem cada vez mais competitivas e lucrativas. Num primeiro momento, os riscos considerados pelas empresas diziam respeito às finanças, logísticas e outras atividades finalísticas.

A partir dos anos 1980, o avanço e a popularização da indústria de informática ocasionaram a migração, no ambiente corporativo, do papel para o computador. Esse novo ambiente, cada vez mais informatizado, trouxe às empresas a necessidade de lidar também como um novo tipo de risco: os riscos à segurança da informação. Apesar da íntima relação da segurança da informação com as tecnologias de informação e comunicação, essa área do conhecimento considera também comportamentos humanos e processos organizacionais, uma vez que também interferem na segurança das informações que se deseja proteger.

Nos últimos anos, a gestão de riscos adquiriu tamanha importância para as empresas que diversos modelos teóricos foram propostos por organizações de renome como o *National Institute of Standards and Technology* (NIST) dos Estados Unidos, *Project Management Institute* (PMI), associação internacional, e a *International Organization for Standardization* (ISO), organização representativa de 170 países responsável por propor e aprovar normas internacionais nos campos técnicos. Não há, todavia, um modelo único a ser aplicado nas empresas, tampouco um melhor modelo para todas elas. Os modelos oferecem abordagens diferentes para a gestão dos riscos e podem ser adequados para uma ou outra empresa, a depender de suas peculiaridades.

Algumas organizações oferecem uma certificação para as empresas que implantarem um modelo de gestão da segurança da informação. A ISO, por exemplo, certifica empresas que desejem implantar o Sistema de Gestão de

Segurança da Informação (SGSI), que abarca também a gestão de riscos. Essa certificação confere maior credibilidade às empresas, sobretudo aquelas cujo negócio esteja relacionado à tecnologia da informação, o que pode lhes trazer novas oportunidades de negócio.

Apesar da importância da gestão de riscos de segurança da informação, muitas empresas ainda não a executam, principalmente aquelas de pequeno porte ou cujo negócio não esteja relacionado às Tecnologias de Informação e Comunicação (TICs). Dentre os fatores que explicam esse comportamento citam-se os custos financeiros e de recursos humanos, a complexidade de implementação dos modelos existentes, falta de percepção das ameaças à segurança da informação, e falta de percepção dos gestores acerca das necessidades e vantagens da gestão de riscos.

O tema desta pesquisa alinha-se à demanda por modelos de gestão de riscos tendo em vista a necessidade das empresas de se protegerem das ameaças à segurança de suas informações. O principal objetivo é propor um modelo de gestão de riscos, inspirado nas recomendações da ISO e com contribuições de outros modelos como o do Nist, que seja simples, prático e flexível, de forma que as empresas possam integrá-lo facilmente às suas atividades técnicas e gerenciais, assegurando assim níveis adequados de segurança para suas informações.

O modelo proposto não esgota as demais abordagens de gestão de riscos de segurança da informação nas organizações. O modelo dirige-se sobretudo às organizações que não possuem experiência nessa área, contribuindo para que a organização adquira experiência e aprimore o processo, ao longo do tempo, de acordo com suas necessidades.

Os objetivos específicos desta pesquisa são:

- Discutir a importância da segurança da informação para as organizações;
- Descrever os principais conceitos da área de Segurança da Informação;
- Descrever os principais conceitos da área de Gestão de Riscos;

- Analisar e descrever as recomendações sobre gestão de riscos de segurança da informação da ISO/IEC 27005:2011;
- Descrever o modelo de gestão de riscos proposto;
- Demonstrar sua aplicação em uma instituição de ensino fictícia.

Para alcançar esses objetivos, em primeiro lugar, há que se proceder à pesquisa bibliográfica focada em Segurança da Informação e Gestão de Riscos. Os modelos de gestão de riscos de segurança da informação da ISO e do Nist também foram pesquisados.

A ISO é hoje uma referência mundial no que concerne às normas técnicas e padrões. É representada no Brasil por meio da Associação Brasileira de Normas Técnicas (ABNT). O Nist é uma organização norte americana congênere à ABNT. Em 2011, publicou, por meio do Laboratório de Tecnologia da Informação, o documento Gerenciando Risco de Segurança da Informação (*Managing Information Security Risk*), no qual propõe um modelo de gestão de riscos com foco em sistemas de informação.

O primeiro capítulo do presente trabalho consolida os principais conceitos da área de Segurança da Informação e Gestão de Riscos, estudados durante a pesquisa bibliográfica.

No capítulo seguinte, serão descritas as recomendações da ISO/IEC 27005, que trata da gestão de riscos de segurança da informação.

No terceiro capítulo, o modelo recomendado pela ISO será analisado criticamente, com o objetivo de verificar melhorias que possam ser aproveitadas no modelo a ser proposto.

No quarto capítulo, será descrito o modelo de gestão de riscos da segurança da informação proposto pela pesquisa e que tem por base o modelo da ISO, com algumas contribuições do modelo do Nist.

Com o objetivo de demonstrar a eficácia e o funcionamento do modelo de gestão de riscos proposto, o mesmo será aplicado em uma instituição de ensino fictícia, por meio do método de investigação denominado estudo de caso. Como sugere Cervo e Bervian (2002), esse método permitirá testar e validar o objeto de estudo, qual seja o modelo de gestão de riscos, de modo que possa evidenciar,

indutivamente, sua aplicabilidade em outras organizações. A aplicação do modelo será descrita no quinto capítulo.

A presente pesquisa soma-se aos esforços teóricos em compreender e discutir a importância da segurança da informação para as organizações, à luz dos principais conceitos da área da Segurança da Informação sobre os quais se sustentará o modelo de gestão de riscos.

Ademais, o modelo proposto permitirá a uma empresa conhecer e analisar as ameaças e vulnerabilidades, e implementar medidas eficazes para reduzir os riscos a níveis aceitáveis, contribuindo para o alcance da missão e objetivos organizacionais. O modelo pretende ser flexível, aplicável a contextos diversos e prático, com o fim de permitir que os gestores possam implementá-lo imediatamente, sem que para isso tenham de despender grandes recursos para sua viabilização.

Por fim, a pesquisa atende às aspirações de seu próprio autor, que na busca por um modelo de gestão de riscos de segurança da informação a ser aplicado na empresa em que trabalha, não encontrou na literatura científica algum que atendesse aos três principais pré-requisitos elencados pelo próprio: simplicidade, flexibilidade e praticidade.

1 CONCEITOS FUNDAMENTAIS

A segurança da informação é hoje considerada consensualmente na literatura científica como de suma importância para as organizações, sejam elas públicas ou privadas. Trata-se de área do conhecimento que se refere à proteção das informações críticas, isto é, aquelas que possuam algum valor para a organização, contra as ameaças. Em primeiro lugar, há que se desconstruir a ideia, comumente veiculada na mídia, de que a segurança da informação visa apenas a preservar as informações contra acesso não autorizado. A confidencialidade de fato é um dos aspectos fundamentais dessa área do conhecimento, mas não o único. Existem outras ameaças tais como interrupção de algum serviço, falha em equipamentos, alteração indevida de dados, e que não estão necessariamente relacionadas ao sigilo das informações.

A segurança da informação abarca também outros dois aspectos, como sugere Adriana Beal (2005, p. 1), e "pode ser entendida como o processo de proteger informações das ameaças à sua integridade, disponibilidade e confidencialidade".

Esses três aspectos da segurança da informação são referenciados na literatura científica como objetivos, requisitos ou princípios da segurança. As medidas de proteção propostas e implementadas na gestão de riscos visam a alcançar e preservar esses três aspectos. Portanto, serão doravante denominados objetivos de segurança. Marcos Sêmola (2003, p. 45, grifo do autor) os define da seguinte forma:

> **Confidencialidade**: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.
>
> **Integridade**: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário visando protegê-las contra alterações indevidas, intencionais ou acidentais.
>
> **Disponibilidade**: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Para alcançar esses objetivos de segurança, torna-se necessário, antes de tudo, conhecer as ameaças e vulnerabilidades a que estão expostos os ativos da

organização; e a probabilidade e o impacto que podem resultar da exploração dessas vulnerabilidades pelas ameaças. Essa análise permite conhecer os riscos aos negócios e identificar e executar as medidas de segurança necessárias para se garantir a continuidade do negócio. Percebe-se, portanto, uma íntima relação entre a segurança da informação e a gestão de riscos, como se pode verificar no conceito proposto por Marcos Sêmola (2003, p. 43): “De forma mais ampla, podemos considerá-la [segurança da informação] como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação”.

A gestão de riscos de segurança da informação pode ser definida, conforme Adriana Beal (2005, p.11), como:

> [...] conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

O Guia ISO 73:2009 afirma, de forma genérica, que a gestão de riscos consiste em atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, entendidos como o efeito da incerteza nos objetivos.

O Nist (2012, p. B-7, tradução do autor), traz um conceito mais técnico ao afirmar que risco é “a medida da extensão para a qual uma entidade é ameaçada por um evento ou circunstância potencial, e tipicamente uma função de: impactos adversos que surgem se uma circunstância ou evento ocorre, e a probabilidade de ocorrência”. A gestão de risco então, segundo essa organização (2012, p. B-8, tradução do autor), consiste em

> processos de planejamento e suporte para gerenciar riscos de segurança da informação para operações organizacionais (incluindo missão, funções, imagem, reputação), ativos organizacionais, indivíduos, outras organizações, e a Nação, e inclui: (i) estabelecimento do contexto para atividades relacionadas a riscos, (ii) avaliação de risco; (iii) resposta aos riscos identificados; e (iv) monitoramento contínuo de risco.

A gestão de riscos é, pois, um processo holístico que engloba todas as atividades, processos e recursos que tenham participação na segurança das informações da empresa. Envolve um estudo aprofundado de todos os ativos e informações que se deseja proteger; identificação de todos os riscos que possam comprometer a segurança desses ativos e informações; implementação de soluções

de segurança de forma a mitigar os riscos identificados a níveis aceitáveis pelos gestores, considerando o impacto que esses riscos podem trazer para a segurança da informação se algum evento adverso ocorrer; e monitoramento contínuo dos riscos.

A gestão de riscos não pode ser confundida com avaliação de riscos. Esse último consiste em uma das etapas do processo de gestão de riscos, como fica claro no conceito trazido elo Nist (2011, p. 37) , segundo o qual a avaliação de riscos (*risk assessment*) “identifica, prioriza e estima os riscos às operações organizacionais [...], ativos organizacionais, indivíduos, outras organizações e a Nação [...]”. A gestão de riscos, por sua vez, consiste num macro-processo, que busca, em primeiro lugar, conhecer os ativos que se deseja proteger e as ameaças que incidem sobre eles. Ademais, envolve a avaliação e implementação de medidas de segurança.

Outro aspecto relevante da gestão de riscos é a iteratividade. A dinamicidade do ambiente corporativo e a constante evolução das TICs exercem influência sobre as variáveis consideradas na identificação dos riscos à segurança da informação. Isso significa que os riscos podem ser alterados a qualquer momento, como por exemplo, se houver a implementação de algum sistema de informação, ou se surgir uma nova ameaça cibernética, ou ainda se o orçamento corporativo para a área de segurança sofrer cortes. Portanto, para que a gestão de riscos seja um processo efetivo, torna-se necessário realizar os processos previstos periodicamente ou sempre que houver uma mudança nas variáveis que afetem os riscos identificados.

Os conceitos referentes aos principais elementos da gestão de riscos serão descritos e criticados na seção seguinte, que trata das recomendações da ISO/IEC 27005 para gestão de riscos de segurança da informação.

2 GESTÃO DE RISCOS – ISO/IEC 27005:2011

A norma ISO/IEC 27005 (2011, p. vi) “fornece diretrizes para o processo de gestão de riscos de segurança da informação”. Essa norma integra a série 27000 da ISO que congrega padrões de segurança da informação e traz recomendações de melhores práticas sobre gestão da segurança da informação, no contexto de um Sistema de Gestão de Segurança da Informação (SGSI).

Segundo a norma ISO/IEC 27001 (2013, p.vi), o SGSI “preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados”.

A norma 27005 propõe um modelo genérico de gestão de riscos, que não esgota as ferramentas de segurança da informação, devendo alinhar-se ao processo maior de gestão de riscos corporativos e integrar-se ao SGSI.

O risco de segurança da informação consiste na combinação da **probabilidade** de que uma **ameaça** possa explorar alguma **vulnerabilidade** de um ativo ou grupo de **ativos de informação**, e as **consequências** que esse **evento** trará para a organização (ISO/IEC, 2009, p.1). A partir dessa assertiva, destacam-se alguns conceitos importantes para a gestão de riscos:

Ativos de informação: informações que possuem valor para a organização e requerem proteção adequada, como por exemplo, contra a perda de sua disponibilidade, confidencialidade e integridade.

Ameaça: ocorrência potencial de um incidente não-desejado, que pode resultar em danos a um sistema ou organização (ISO/IEC, 2014, p.11).

Vulnerabilidade: fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças (ISO/IEC, 2014, p.12)

Consequência: resultado de um evento que afeta os objetivos (ABNT, 2009, p. 5). Pode ter efeitos positivos ou negativos sobre os objetivos da organização. A norma ISO/IEC 27005 também faz referência ao termo impacto, que apesar de parecer sinônimo de consequência, difere-se deste por ser mais

abrangente e relacionar-se diretamente ao sucesso de um incidente envolvendo a segurança da informação (ABNT, 2011, p. 51).

Evento: ocorrência ou mudança em um conjunto específico de circunstâncias (ABNT, 2009, p.4). Pode ser referido também como incidente ou acidente.

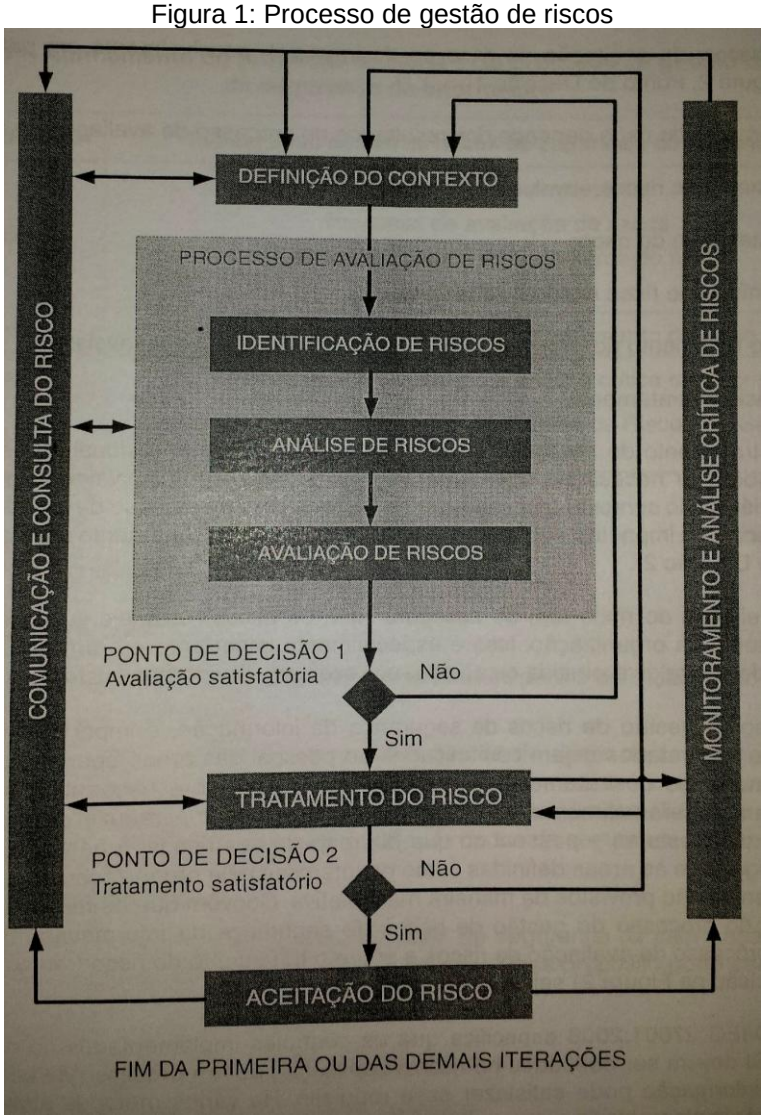
Probabilidade: medida de chance de ocorrência expressa como um número entre 0 e 1, onde 0 é a impossibilidade e 1 é a certeza absoluta.

Os demais conceitos acerca da gestão de riscos serão abordados no decorrer da descrição das recomendações da norma ISO/IEC 27005.

2.1 Processo de Gestão de Riscos

O processo de gestão de riscos, previsto na norma ISO/IEC 27005, deve ser aplicado de forma contínua, podendo abarcar toda ou parte da organização. Conforme Figura 1, consiste nas seguintes etapas: 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.

Figura 1: Processo de gestão de riscos



Fonte - ABNT (2011, p.9)

Em primeiro lugar, procede-se ao levantamento do contexto. Após, inicia-se o processo de avaliação de riscos que envolve três fases: identificação, análise e avaliação de riscos. Se o processo de avaliação for considerado insatisfatório, poderão ser feitas quantas iterações forem necessárias para que os riscos possam ser estimados e avaliados adequadamente, reduzindo o tempo e esforço necessários na identificação de controles de segurança.

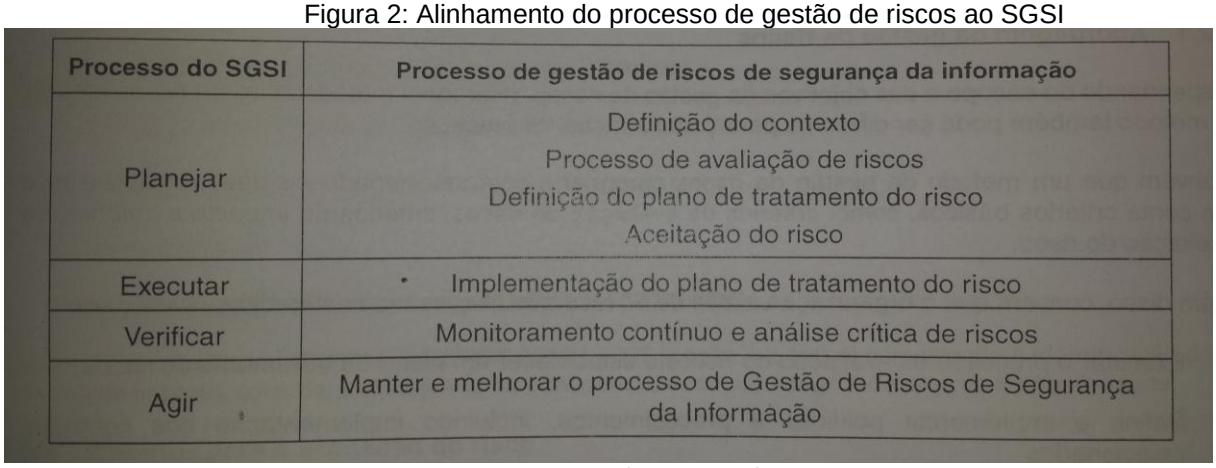
Considerada satisfatória a avaliação dos riscos, procede-se à etapa seguinte qual seja a do tratamento dos riscos, em que se determinam as ações necessárias para reduzir os riscos a níveis aceitáveis. Essa etapa também pressupõe um processo iterativo. Avalia-se o tratamento do risco e decide-se se os níveis de risco residual são aceitáveis. Caso os resultados não sejam satisfatórios,

retorna-se à fase da definição do contexto para alterar alguns critérios como por exemplo os de aceitação do risco, e em seguida para a fase da avaliação dos riscos. O ciclo só está concluído após aceitação pelos gestores da organização dos riscos residuais.

As informações sobre os riscos e as medidas de segurança implementadas para mitigá-los devem ser comunicadas aos gestores e colaboradores que tenham participação na segurança da informação, independente da fase do processo de gestão de riscos. Essa comunicação contínua contribui para o gerenciamento de incidentes e eventos não previstos de forma mais eficiente.

O processo de gestão de riscos coaduna-se com SGSI, proposto na norma ISO/IEC 27001 e baseado no método de gestão PDCA, acrônimo que representa as seguintes atividades, em inglês: *plan* (planejar), *do* (executar), *check* (verificar) e *act* (agir). A figura 2 relaciona o processo de gestão de riscos ao SGSI.

Figura 2: Alinhamento do processo de gestão de riscos ao SGSI



Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Fonte – ABNT (2011, p.11).

As etapas previstas no processo de gestão de riscos serão descritas nas subseções seguintes.

2.1.1 *Definição do contexto*

Na primeira etapa, o contexto em que será realizada a gestão de riscos é definido por meio da especificação dos critérios básicos, o escopo e limites do processo de gestão de riscos e a organização do processo.

2.1.1.1 Critérios Básicos

Os critérios básicos definidos nessa fase serão utilizados como parâmetro para a etapa do processo de avaliação de riscos. São definidos três tipos de critérios.

- Critérios para avaliação de riscos: são utilizados para avaliar os riscos identificados e especificar as prioridades para o tratamento dos riscos. Devem considerar o valor estratégico do processo que trata as informações de negócio; a criticidade dos ativos de informação envolvidos; requisitos legais e regulatórios, bem como as obrigações contratuais; importância, do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade; expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado, a imagem e reputação da organização (ABNT, 2011, p. 12).
- Critérios de impacto: são especificados em função dos danos ou custos à organização causados por um evento relacionado com a segurança da informação e são utilizados como parâmetros na análise de riscos. Devem levar em conta o nível de classificação do ativo de informação afetado; ocorrência de violação da segurança da informação; operações comprometidas; perda de oportunidades de negócio e de valor financeiro; interrupção de planos e o não cumprimento de prazos; danos à reputação; e violações de requisitos legais, regulatórios ou contratuais.
- Critérios para aceitação do risco: dependem das políticas, metas e objetivos da organização, e das partes interessadas. São utilizados pelos gestores para decidirem acerca dos níveis de riscos aceitáveis e devem considerar os critérios de negócio; aspectos legais e regulatórios; operações; tecnologia; finanças; e fatores sociais e humanitários.

2.1.1.2 Escopo e limites

Nessa subetapa, são reunidas informações que possam determinar o ambiente em que a organização opera e de que forma ele afeta o processo de gestão de riscos. O escopo refere-se à abrangência em que será realizada a gestão de riscos e os limites dizem respeito aos aspectos do ambiente interno e externo à organização e que irão interferir nesse processo.

As informações necessárias para definição do escopo e limites são: objetivos estratégicos; políticas e estratégias; processos de negócio; funções e estrutura da organização; requisitos legais, regulatórios e contratuais aplicáveis à organização; Política de Segurança da Informação (PSI), se houver; abordagem da organização à gestão de riscos; ativos de informação; localidades em que a organização se encontra e suas características geográficas; restrições que afetam a organização; expectativas das partes interessadas; ambiente sociocultural; e interfaces, ou seja, a troca de informação com o ambiente (ABNT, 2011, p.14).

2.1.1.3 Organização para gestão de riscos de segurança da informação

Nessa subetapa são estabelecidas as responsabilidades e a forma como será organizado o processo de gestão de riscos. Os principais papéis e responsabilidades dessa organização são: desenvolvimento do processo de gestão de riscos adequado à organização; identificação e análise das partes interessadas; definição dos papéis e responsabilidades de todas as partes, internas e externas à organização; estabelecimento das relações necessárias entre a organização e as partes interessadas, das interfaces com as funções de alto nível de gestão de riscos da organização, assim como das interfaces com outros projetos ou atividades relevantes; definição de alçadas para a tomada de decisões; e especificação dos registros a serem mantidos (ABNT, 2011, p.15).

2.1.2 *Processo de avaliação de riscos*

O processo de avaliação de riscos envolve a identificação, quantificação ou descrição qualitativa, e priorização dos riscos em função dos critérios de avaliação e dos objetivos relevantes da organização definidos na etapa anterior.

A norma sugere que esse processo seja realizado em duas ou mais iterações. Na primeira, realiza-se uma avaliação de alto nível para identificar riscos potencialmente altos, os quais merecem uma avaliação mais aprofundada, realizada na segunda iteração. Poderão ser realizadas tantas iterações quanto forem necessárias para que sejam coletadas informações suficientes para uma análise aprofundada dos riscos.

O processo de avaliação de riscos consiste nas seguintes subetapas: identificação de riscos, análise de riscos e avaliação de riscos.

2.1.2.1 Identificação de riscos

O propósito dessa subetapa é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer(ABNT, 2011, p.16). Consiste nas seguintes atividades: identificação dos ativos; identificação das ameaças; identificação dos controles existentes; identificação das vulnerabilidades; e identificação das consequências.

2.1.2.1.1 Identificação de ativos

Trata-se de atividade que visa a listar todos os ativos que possuem valor para a organização e cujos riscos deverão ser gerenciados. A identificação dos ativos deve ser suficientemente detalhada para permitir uma adequada avaliação dos riscos.

A norma propõe que para cada ativo seja designado um responsável, mesmo que ele não tenha propriedade sobre ele. Isso garante a prestação de contas pelo responsável sobre o ativo sob sua tutela.

Os ativos podem ser distinguidos em primários e de suporte e infraestrutura, conforme o quadro 1.

Quadro 1: Ativos primários e ativos de suporte e infraestrutura

Ativos primários	Ativos de suporte e infraestrutura
•Processos e atividades do negócio •Informação	• Hardware • Software • Rede • Recursos Humanos • Instalações Físicas • Estrutura da organização

Fonte – ABNT (2011, p.41).

Os ativos primários consistem nos principais processos e informações das atividades incluídas no escopo. Esses ativos são considerados vitais para a organização. Os ativos de suporte são aqueles que apresentam vulnerabilidades que podem ser exploradas por ameaças cujo objetivo é comprometer os ativos primários (ABNT, 2011, p.41).

2.1.2.1.2 Identificação das ameaças

As ameaças podem surgir de dentro ou fora da organização e comprometer um ou mais ativos. Podem ser de origem natural ou humana (acidentais ou intencionais). Os dados a respeito das ameaças podem ser obtidos a partir da análise crítica de incidentes, dos responsáveis pelos ativos, usuários, catálogos de ameaças, especialistas em segurança, entre outros.

O produto obtido nessa atividade é uma lista de ameaças com a identificação do tipo e da fonte das ameaças.

2.1.2.1.3 Identificação dos controles existentes

Para a ISO/IEC 27005 (2011, p. 2), controle é a medida que está modificando o risco e inclui qualquer processo, política, procedimentos, diretriz, prática ou estrutura organizacional, que pode ser de natureza administrativa, técnica, gerencial ou legal. Os controles já implementados devem ser identificados e avaliados de forma a assegurar que estejam funcionando adequadamente. Os controles ainda não implementados, a exemplo daqueles previstos nos planos de tratamento de risco, também devem ser avaliados com relação à sua efetividade.

Os controles podem ser ineficazes, insuficientes ou não justificados, o que pode suscitar o surgimento de vulnerabilidades. O produto final desta atividade é uma lista de todos os controles existentes e planejados, sua implementação e status de utilização.

2.1.2.1.4 Identificação das vulnerabilidades

Para identificar as vulnerabilidades que podem ser exploradas, comprometendo os ativos, é necessário conhecer as ameaças, os ativos e os controles existentes. O risco só existe quando uma vulnerabilidade pode ser explorada por uma ameaça ou, inversamente, uma ameaça possa explorar alguma vulnerabilidade. Controles ineficazes por si só podem ser considerados vulnerabilidades.

As vulnerabilidades podem ser identificadas nas seguintes áreas: organização; processos e procedimentos; rotinas de gestão; recursos humanos; ambiente físico; configuração do sistema de informação; *hardware*, *software* ou equipamentos de comunicação; e dependência de entidades externas (ABNT, 2011, p.16).

Para identificar vulnerabilidades técnicas, a norma sugere métodos pró-ativos como ferramentas automatizadas de procura por vulnerabilidade, avaliação e testes de segurança, teste de invasão e análise crítica de código.

2.1.2.1.5 Identificação das consequências

As consequências que podem resultar de um cenário de incidente e comprometerem a confidencialidade, integridade e disponibilidade dos ativos devem ser identificadas. Um cenário de incidente é a descrição de uma ameaça explorando uma vulnerabilidade ou um conjunto de vulnerabilidades resultando em um incidente de segurança da informação (ABNT, 2011, p.20).

Nessa atividade, o objetivo é produzir uma lista de cenários de incidentes com suas consequências, associadas aos ativos e processos de negócio. A estimativa dos impactos dos cenários deve considerar essas consequências bem como os critérios de impacto estabelecidos na etapa da definição do contexto.

As organizações devem identificar as consequências operacionais dos cenários de incidentes em função de (mas não limitado a): investigação e tempo de reparo; tempo perdido; oportunidade perdida; saúde e segurança; custo financeiro das competências específicas necessárias para reparar o prejuízo; imagem, reputação e valor de mercado (ABNT, 2011, p.20).

2.1.2.2 Análise de riscos

Análise de risco, segundo a norma ISO/IEC 27005 (2011, p. 4), consiste no processo de compreender a natureza do risco e determinar o nível de risco, fornecendo a base para a avaliação dos riscos e para as decisões sobre o tratamento de riscos.

Na subetapa de análise de riscos, em primeiro lugar, deve ser escolhida uma metodologia de análise que pode ser qualitativa ou quantitativa, ou ainda uma combinação de ambas.

A análise qualitativa, apesar de mostrar-se mais subjetiva que a quantitativa, é menos complexa e envolve atributos que indicam a magnitude das consequências de um incidente e a probabilidade de ocorrência dessas consequências. Esse método de análise pode ser utilizado (i) como uma verificação inicial a fim de identificar riscos que exigem uma análise mais detalhada; (ii) quando esse tipo de análise é suficiente para a tomada de decisões; (iii) ou quando os dados numéricos ou recursos são insuficientes para uma análise quantitativa (ABNT, 2011, p.21).

A análise quantitativa envolve escalas numéricas para indicar as consequências e a probabilidade. A vantagem desse método está na exatidão da avaliação dos riscos e dos valores associados a eles. Por outro lado, ocorre que nem sempre os dados necessários à análise quantitativa estão disponíveis, o que compromete sua eficiência metodológica.

Após escolha do método de análise de riscos, são realizadas as atividades de avaliação das consequências, avaliação da probabilidade dos incidentes e a determinação do nível de risco.

2.1.2.2.1 Avaliação das consequências

Nessa atividade, avaliam-se os impactos causados por incidentes relacionados à segurança da informação e que possam comprometer a confidencialidade, integridade e disponibilidade dos ativos.

Antes de avaliar as consequências, é importante que se proceda à valoração dos ativos identificados na subetapa da identificação dos riscos.

A valoração classifica os ativos segundo sua importância para a realização dos objetivos de negócio da organização. É realizada com base em uma escala de medida, que pode ser qualitativa ou quantitativa, e em critérios que permitam ordená-los em função de sua importância para a organização. Esses critérios podem ser baseados no custo original do ativo, no custo de sua substituição, no valor da reputação para a organização, entre outros. Para que a valoração dos ativos tenha um denominador comum, a norma sugere que os critérios sejam utilizados para estimar as possíveis consequências resultantes da perda de confidencialidade, integridade, disponibilidade, assim como da capacidade de garantir o não-repúdio, a responsabilização, a autenticidade e a confiabilidade (ABNT, 2011, p.22).

As consequências podem ser determinadas por meio da criação de modelos com os resultados de um evento, um conjunto de eventos ou por meio da extrapolação a partir de estudos experimentais ou dados passados (ABNT, 2011, p.22).

O produto dessa atividade é uma lista de consequências avaliadas segundo critérios de impacto, associadas aos ativos e relacionadas a um cenário de incidente.

2.1.2.2.2 Avaliação da probabilidade dos incidentes

Probabilidade, segundo a norma ISO/IEC 27005 (2011, p. 3), é a chance de algo acontecer. Portanto, nessa atividade avalia-se a chance dos cenários de incidentes acontecerem.

A avaliação pode ser qualitativa ou quantitativa e deve levar em conta: a experiência passada e as estatísticas aplicáveis referentes à probabilidade da

ameaça; a motivação e as competências, que mudam ao longo do tempo, os recursos disponíveis para possíveis atacantes, bem como a percepção da vulnerabilidade e o poder da atração dos ativos para um possível atacante, quando se tratar de fontes de ameaças intencionais; fatores geográficos, possibilidade de eventos climáticos extremos e fatores que poderiam acarretar erros humanos e mau funcionamento de equipamentos, quando se tratar de fontes de ameaças acidentais; vulnerabilidades; e controles existentes e a eficácia com que eles reduzem as vulnerabilidades (ABNT, 2011, p.23).

2.1.2.2.3 Determinação do nível de risco

O objetivo dessa atividade é estimar o risco para todos os cenários de incidentes relevantes, combinando a probabilidade de um cenário e as suas consequências.

Existem diversos métodos que fazem uso de tabelas e matrizes que combinam medidas empíricas com medições subjetivas. A norma sugere que a organização faça uso do método com o qual se sinta confortável. A figura 3 ilustra um método qualitativo sugerido pela norma e que combina o valor do ativo, a probabilidade de ocorrência de uma ameaça e a facilidade de exploração do ativo por essa ameaça, gerando uma medida de risco em escala de 0 a 8.

Figura 3: Matriz de análise de risco

	Probabilidade da ocorrência – Ameaça	Baixa			Média			Alta		
	Facilidade de Exploração	B	M	A	B	M	A	B	M	A
Valor do Ativo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Fonte – ABNT (2011, p.68).

2.1.2.3 Avaliação de riscos

Nessa subetapa, comparam-se os níveis dos riscos estimados na subetapa anterior com os critérios de avaliação de riscos e com os critérios para aceitação do risco definidos na etapa da definição de contexto.

Segundo a Norma da ABNT (2011, p. 24), a avaliação de riscos deve considerar:

- Propriedade da segurança da informação: se um critério não for relevante para a organização, logo todos os riscos que provocam esse tipo de impacto podem ser considerados irrelevantes;
- Importância do processo de negócios ou da atividade suportada por um determinado ativo ou conjunto de ativos: se o processo for considerado de baixa importância, convém que os riscos associados a ele sejam menos considerados que os riscos que causam impactos em processos ou atividades mais importantes.

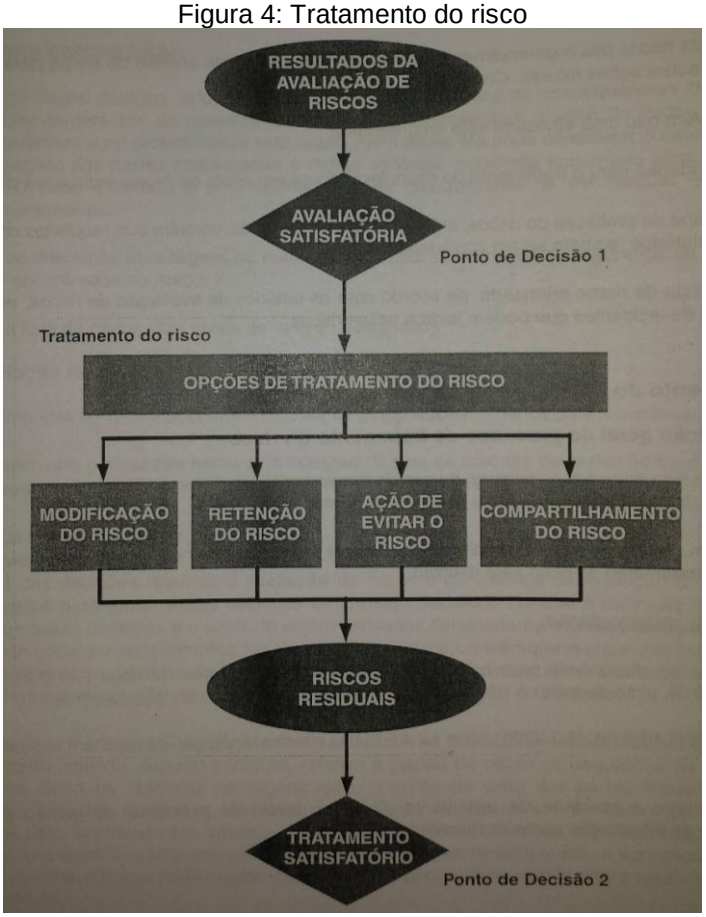
As decisões acerca da avaliação de riscos devem estabelecer prioridades para o tratamento dos riscos, de acordo com os critérios de avaliação dos riscos. Ao final dessa subetapa, tem-se uma lista com os riscos priorizados em relação aos cenários de incidentes que podem levar a esses riscos.

2.1.3 Tratamento do risco de segurança da informação

O objetivo dessa etapa é definir um plano de tratamento de riscos com base em quatro opções: modificação, retenção, ação de evitar e compartilhamento do risco (Figura 4). Esse plano deve indicar uma ou mais opções de tratamento, em ordem de prioridade, para cada risco identificado, assim como seus prazos de execução. A opção pela forma de tratamento deve levar em conta como o risco é percebido pelas partes interessadas e as formas mais apropriadas de comunicação com as partes (ABNT, 2011, p.27).

A escolha da opção deve pautar-se no resultado do processo de avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos. A premissa dessa etapa é reduzir ao mínimo possível as consequências negativas que o risco pode trazer.

Figura 4: Tratamento do risco



Fonte – ABNT (2011, p.26).

Após definido o plano de tratamento, deve-se estabelecer os riscos residuais, por meio de uma atualização ou iteração do processo de avaliação de riscos. Os riscos residuais serão analisados na etapa da aceitação do risco, na qual as decisões serão baseadas em critérios definidos na primeira etapa da definição de contexto.

2.1.3.1 Modificação do risco

O risco pode ser modificado por meio da inclusão, exclusão ou alteração de controles, de forma que o risco residual possa ser reduzido e, por conseguinte, aceito. Os controles selecionados devem satisfazer os critérios para aceitação do risco e os requisitos legais, regulatórios e contratuais. Devem considerar também custos, prazos, interação com outros controles, aspectos técnicos, culturais e ambientais, e demais restrições que possam afetar sua implementação.

Segundo a norma ISO/IEC 27005 (2011, p. 28), os controles, em geral, fornecem os seguintes tipos de proteção: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização.

2.1.3.2 Retenção do risco

A retenção do risco ocorre quando se aceita o risco, de forma consciente e objetiva, sem o tratamento específico, ou seja, dispensando a implementação de controles adicionais. O nível do risco aceito, todavia, deve satisfazer os critérios para a aceitação do risco.

2.1.3.3 Ação de evitar o risco

Quando as outras opções de tratamento de risco se mostram onerosas e os riscos demasiadamente elevados, pode-se optar pela ação de evitar o risco, ou seja, evitar a condição que dá origem ao risco. Pode-se, por exemplo, eliminar ou suspender uma atividade planejada ou existente, ou ainda alterar as condições em que essa atividade ocorra de modo a evitar o risco.

2.1.3.4 Compartilhamento do risco

A quarta opção de tratamento do risco diz respeito ao compartilhamento dos riscos com entidades externas à organização, como por exemplo, seguradoras, que cubram as consequências de um incidente, ou empresa de monitoramento de sistemas de informação cuja responsabilidade é impedir ataques cibernéticos. O compartilhamento do risco deve considerar a avaliação dos riscos e se torna conveniente quando a entidade externa mostra-se capaz de melhor gerenciar o risco. Essa opção pode criar novos riscos ou modificar riscos existentes e identificados, o que pode demandar novo tratamento de risco.

2.1.4 Aceitação do risco

Nessa etapa, os gestores devem realizar uma análise crítica, aprovar, se for o caso, os planos propostos de tratamento do risco e os riscos residuais resultantes, e registrar as condições para essa aprovação.

A aceitação do risco deve ser formalmente registrada e considerar os critérios definidos na etapa inicial do processo de gestão de riscos. O produto final dessa etapa é uma lista de riscos aceitos, com uma justificativa dos gestores para aqueles que não atendam os critérios de aceitação de riscos.

2.1.5 Comunicação e consulta do risco

A comunicação e consulta do risco não constituem uma etapa em si do processo de gestão de riscos de segurança da informação, mas uma atividade bidirecional que deve ser continuamente executada com o objetivo de promover e disseminar o entendimento acerca de como os riscos devem ser gerenciados.

Essa atividade consiste no compartilhamento de informações entre os tomadores de decisão e as demais partes interessadas no processo de gestão de riscos. Como os atores desse processo podem ter percepções distintas sobre os riscos, o compartilhamento de informações sobre os riscos pode contribuir para sua gestão. As organizações devem elaborar planos de comunicação dos riscos para situações cotidianas e para situações emergenciais, como no caso de um incidente.

O objetivo da comunicação do risco deve: fornecer garantia do resultado da gestão de riscos; coletar informações sobre os riscos; compartilhar os resultados do processo de avaliação de riscos e apresentar o plano de tratamento; evitar ou reduzir tanto a ocorrência quanto as consequências das violações da segurança da informação que aconteçam devido à falta de entendimento mútuo entre os tomadores de decisão e as partes interessadas; dar suporte ao processo decisório; obter novo conhecimento sobre a segurança da informação; coordenar com as outras partes e planejar respostas para reduzir as consequências de um incidente; dar aos tomadores de decisão e às partes interessadas um senso de responsabilidade sobre riscos; e melhorar a conscientização (ABNT, 2011, p.31).

2.1.6 Monitoramento e análise crítica de riscos

Os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) podem alterar a qualquer momento. Isso torna necessário o monitoramento contínuo com o objetivo de detectar mudanças que possam afetar negativamente a organização.

A norma ISO/IEC 27005 (2011, p. 32) sugere que a organização monitore continuamente os seguintes itens:

- Novos ativos que tenham sido incluídos no escopo da gestão de riscos;
- Modificações necessárias dos valores dos ativos, por exemplo, devido à mudança nos requisitos de negócio;
- Novas ameaças que podem estar ativas tanto fora quanto dentro da organização e que não tenham sido avaliadas;
- Possibilidade de que vulnerabilidades novas ou ampliadas venham a permitir que alguma ameaça as explore;
- Vulnerabilidades já identificadas, para determinar aquelas que estão se tornando expostas a ameaças novas ou ressurgentes;
- Consequências ou impacto ampliado de ameaças, vulnerabilidades e riscos avaliados em conjunto, em um todo agregado, resultando em um nível inaceitável de risco;
- Incidentes relacionados à segurança da informação.
- Qualquer mudança que afete a organização, seja nos riscos em si, em um de seus fatores, ou ainda no próprio contexto da organização, deve ser analisada criticamente para evitar que riscos sejam subestimados ou mesmo omitidos.

Com o monitoramento dos riscos, espera-se maior alinhamento da gestão de riscos com os objetivos da organização.

2.1.7 Monitoramento, análise crítica e melhoria do processo de gestão de riscos

Além dos riscos e seus fatores, o processo de gestão de riscos, como um todo, também deve ser continuamente monitorado e analisado criticamente, de forma que o contexto, o processo de avaliação de riscos e o tratamento do risco continuem relevantes e adequados para a organização.

O monitoramento e análise crítica devem abarcar: o contexto legal e ambiental; o contexto da concorrência; a abordagem do processo de avaliação de riscos; o valor e categorias dos ativos; os critérios de impacto; os critérios para avaliação de riscos; os critérios para aceitação do risco; o custo total de propriedade; e os recursos necessários (ABNT, 2011, p.33).

Essas duas atividades podem demandar mudanças na abordagem, metodologia ou ferramentas no processo de gestão de riscos. O resultado esperado é a garantia da atualização e relevância desse processo para os objetivos de negócio da organização.

3 ANÁLISE CRÍTICA DA ISO/IEC 27005:2011

Antes de proceder à descrição do modelo proposto por esta pesquisa, é preciso tecer algumas considerações acerca do processo de gestão de riscos recomendado pela ISO/IEC 27005:2011. Esse exercício crítico busca identificar aspectos que possam ser alterados e/ou simplificados com objetivo de se alcançar um modelo mais prático para pronta implementação nas organizações.

A Segurança da Informação refere-se à atividade de proteger as informações contra as ameaças à sua integridade, disponibilidade e confidencialidade. O processo de gestão de riscos de segurança de informação tem como objetivo imediato conhecer e tratar os riscos às informações consideradas valiosas pela organização.

Vê-se, portanto, que conhecer as informações e o valor que possuem para a organização é a atividade base do processo de gestão de riscos. Isso significa que as demais atividades previstas devem sempre referir-se diretamente a algum ativo. Quando as atividades são executadas sem essa referência, é possível que o processo perca o foco, como por exemplo, considerar ameaças e vulnerabilidades que não afetem a segurança de ativo que possua valor para a organização; mais ainda, pode ocorrer a proposição de controles que não surtirão efeito algum na proteção dos ativos que de fato requerem medidas de segurança.

A primeira etapa do modelo da ISO prevê a atividade de estabelecimento de critérios básicos para a avaliação de riscos, de impacto, e para a aceitação de risco. Em primeiro lugar, ao se estabelecerem os critérios no início do processo, é possível que aspectos importantes sejam omitidos uma vez que, nessa fase, poucas informações foram coletadas a respeito dos riscos à segurança da informação. Ademais, reservar à organização a tarefa de definir os critérios de avaliação de risco e de impacto pode ser complexa, principalmente quando não há qualquer abordagem implementada de gestão de riscos de segurança da informação.

Os critérios de aceitação de risco, por sua vez, podem ser dispensáveis. O princípio que deve nortear a gestão de riscos é minimizar tanto quanto possível o nível dos riscos identificados, cabendo aos gestores avaliar e aprovar o tratamento de risco proposto, ou aceitá-lo ou compartilhá-lo, mediante justificativa. Assim, a

decisão dos gestores acerca da aceitação ou não de risco é inerentemente discricionária e circunstancial, dispensando, pois, a definição prévia de critérios para aceitação.

A despeito da análise de riscos, a norma ISO/IEC 27005 não sugere uma metodologia específica para avaliação das consequências, probabilidade e determinação do nível de risco. O Anexo E da norma deixa claro que a organização deverá usar um método com o qual se sinta confortável e descreve alguns exemplos de métodos que combinam medidas empíricas com medições subjetivas. Isso dificulta a implementação do processo de gestão de riscos principalmente por parte daquelas organizações que não possuem experiência seja em gestão de riscos ou em segurança da informação.

De forma geral, o modelo proposto nesta pesquisa busca redistribuir e sintetizar algumas atividades recomendadas pela ISO/IEC 27005. Busca também estabelecer abordagens e parâmetros para a avaliação de riscos, de forma a facilitar a implementação do processo de gestão de riscos nas organizações.

Vale lembrar que o modelo proposto não esgota as demais abordagens de gestão de riscos de segurança da informação nas organizações. O objetivo do modelo é constituir-se uma ferramenta de fácil implementação para aquelas organizações que não possuem experiência nessa área, contribuindo para que a organização adquira experiência e aprimore o processo, ao longo do tempo, de acordo com suas necessidades.

4 MODELO PRÁTICO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O modelo prático de gestão de riscos de segurança da informação tem como objetivo assegurar a disponibilidade, confidencialidade e integridade de todas as informações que possuem valor para uma organização. Para tanto, o modelo prevê um processo holístico e iterativo, que abarca todas as variáveis que afetam a segurança de um ativo de informação, sejam elas recursos, processos, dispositivos de tecnologia da informação, pessoas, entre outros.

Esse modelo permite à organização conhecer e distinguir as informações valiosas para seu negócio. Não se trata se informações comerciais que representem oportunidades de negócio, mas das informações que a organização possui e cuja perda de sua disponibilidade, confidencialidade e/ou integridade pode resultar em prejuízos à organização. Por esse motivo, o processo de gestão de riscos deve estar continuamente alinhado aos objetivos da organização, de forma que possa efetivamente contribuir para a prosperidade e continuidade do negócio.

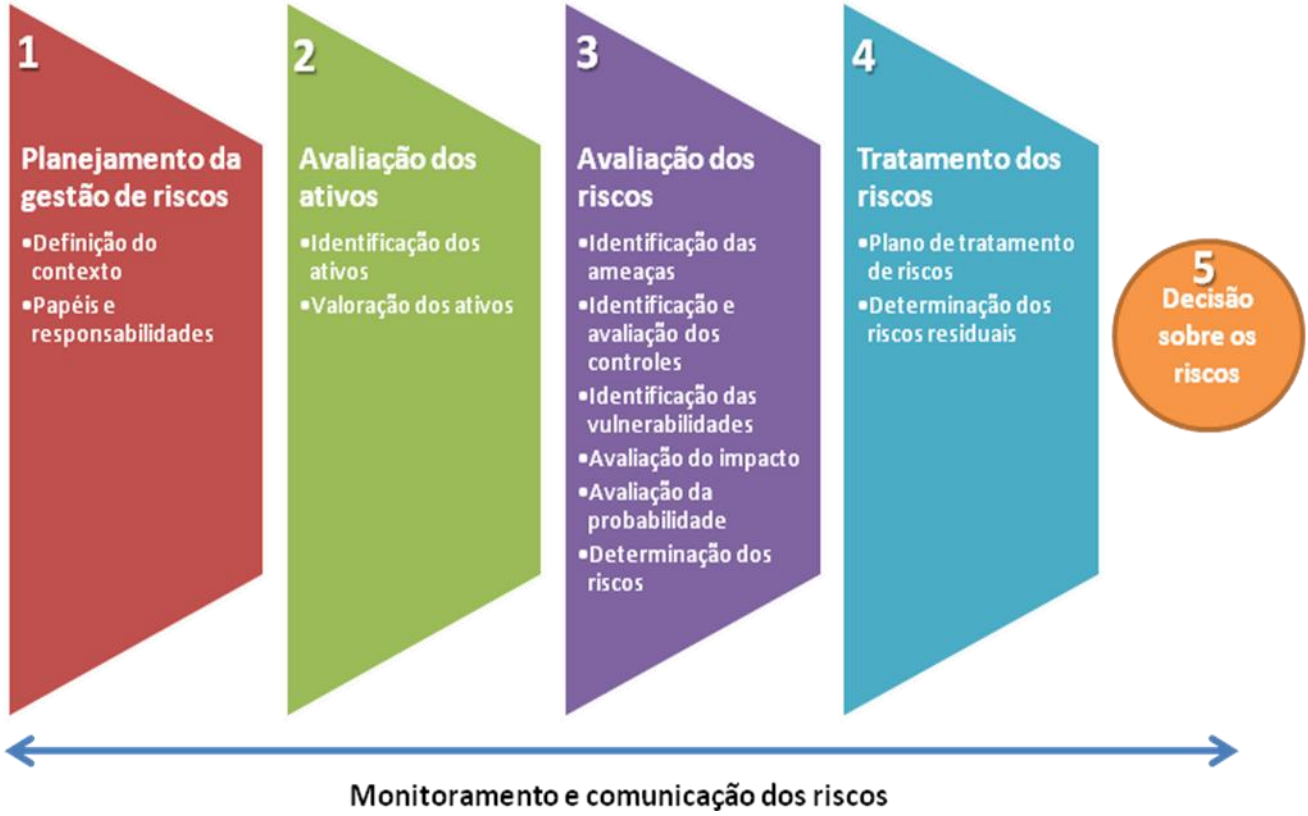
Ademais, o modelo permitirá conhecer as ameaças que incidem sobre os ativos de informações; detectar vulnerabilidades relacionadas a esses ativos; identificar a probabilidade e o impacto dessas ameaças explorarem as vulnerabilidades; estimar os riscos associados aos ativos; avaliá-los; e tratá-los por meio de soluções de segurança. O processo de gestão de riscos deve ser incluído na rotina da organização e executado de forma cíclica e iterativa, garantindo um monitoramento contínuo da segurança dos ativos de informação e uma resposta eficiente no caso da alteração de alguma variável que possa afetar os riscos já identificados. Deve também integrar-se às demais atividades da organização, pois os ativos de informação e os demais fatores do risco, em geral, encontram-se diluídos por todo o ambiente corporativo. O processo, portanto, envolve uma ampla gama de colaboradores da organização e não apenas aqueles que lidam com a gestão da segurança da informação.

O público alvo desse modelo são as organizações que ainda não possuem um processo de gestão de riscos da segurança da informação implementado ou que ainda não tenham experiência nessa área. O processo de gestão de riscos proposto automatiza algumas atividades, ao contrário das

recomendações da ISO, que sugerem que as organizações desenvolvam abordagens próprias para determinadas atividades, como, por exemplo, a avaliação de riscos. Dessa forma, a expectativa é de que a organização possa utilizá-lo como um primeiro passo para implementação da gestão de riscos de segurança da informação e aprimorá-lo à medida que adquirir experiência nessa área.

Conforme Figura 5, o modelo de gestão de riscos prevê o seguinte processo:

Figura 5: Proposta de processo de gestão de riscos



Fonte: Produzido polo autor do presente trabalho.

4.1 Planejamento da gestão de riscos

A primeira etapa da gestão de riscos consiste nas atividades de definição de contexto e na delimitação dos papéis e responsabilidades.

Vale lembrar que a ISO 27005 prevê, na primeira etapa do processo de gestão de riscos, a definição de critérios de impacto, de avaliação de riscos e de aceitação de riscos. Contudo, no modelo proposto, os critérios necessários para a

avaliação das variáveis de risco serão pré-definidos e descritos no decorrer da exposição do modelo.

4.1.1 Definição do contexto

A definição do contexto envolve a coleta de dados a respeito da organização para que se possa alinhar o modelo proposto de gestão de riscos da segurança da informação à identidade da organização. Os principais dados necessários para definição do contexto para a gestão de riscos são definidos a seguir. No entanto, deverão também ser contemplados os demais dados não listados aqui e que a organização julgue contribuir para determinar o ambiente organizacional e a relevância desse ambiente para a gestão de riscos.

Negócio: diz respeito à principal atividade ou área de atuação da organização.

Visão: refere-se à autoimagem da organização e descreve, de forma simples e objetiva, como ela pretende se ver no futuro ou o que ele pretende ser (COSTA, 2002, p. 35).

Missão: refere-se à razão da existência da organização e define o seu propósito fundamental.

Valores: características, virtudes, qualidades da organização (COSTA, 2002, p. 38). Representa as convicções dominantes em que a maioria das pessoas da organização acredita.

Objetivos estratégicos: estão estreitamente ligados à missão e consistem em valores quantitativos e qualitativos que a organização pretende atingir ou manter.

Organograma: é a representação gráfica da estrutura da organização. Convém detalhar as atribuições e competências de cada área representada no organograma, bem como a forma como essas áreas se relacionam. Convém ainda detalhar as áreas que tratam com segurança da informação ou com informática.

Localidade e características geográficas: descrição de onde está sediada a organização, bem como do local de suas filiais, se houver. Convém fazer um breve relato do ambiente físico externo no qual estão localizadas as unidades,

com o objetivo de contribuir para definição do escopo do processo de gestão de riscos.

Aspectos legais e contratuais: descrição de todas as condições que sujeitam a organização a obrigações legais e contratuais, sobretudo aquelas que irão interferir na disponibilidade, integridade e confidencialidade de suas informações.

Segurança da Informação: convém verificar se a instituição dispõe da Política de Segurança da Informação (PSI), documento formal, estabelecido pela alta direção e que inclui os objetivos de segurança da informação e o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação (ABNT, 2013, p.3). Caso a organização não disponha desse documento, convém descrever os principais objetivos de segurança da informação ou a percepção da organização acerca dessa área.

Expectativas das partes interessadas: todos aqueles (pessoas ou organizações) que podem afetar, ser afetados, ou perceber-se afetados por uma decisão ou atividade. Convém descrever como se dá o envolvimento dessas partes com a gestão de riscos e o que podem esperar desse processo.

Restrições: aspectos que afetam a organização e determinam o direcionamento da segurança da informação (ABNT, 2011, p. 36). Podem ser de natureza diversa a exemplo de restrições orçamentárias, políticas, técnicas, ambientais, entre outras.

Objetivo da gestão de riscos: definir qual o propósito e abrangência (escala e frequência) da gestão de riscos. É possível limitá-la a uma unidade específica da organização, a um departamento, a um grupo de ativos, ou ainda, pode ser limitada por um período de tempo ou pode ser implementada de forma permanente.

4.1.2 Papéis e responsabilidades

Para que as atividades previstas no processo de gestão de riscos sejam realizadas de forma eficiente, torna-se necessário definir previamente as principais funções que atuam diretamente nesse processo e designar os colaboradores que executarão essas funções.

Gestor de riscos de segurança da informação: pessoa ou equipe responsável por acompanhar o processo de gestão de riscos de segurança da informação desde o início. É responsável por reunir todas as informações coletadas durante o processo e assegurar o devido andamento das atividades. Ademais, cabe a ele fazer o contato e aproximar os diversos atores que atuam, direta ou indiretamente, na gestão de riscos.

Analista de riscos de segurança da informação: é aquele que preenche as listas de verificação, busca dados específicos, e executa as demais atividades operacionais previstas no processo de gestão de riscos. Reporta-se diretamente ao gestor de riscos, o qual pode delegar-lhe funções relacionadas à segurança da informação. Auxilia também o proprietário do risco por meio de atividades operacionais.

Proprietário do ativo de informação: pessoa ou entidade responsável pelo ciclo de vida de um ativo. O proprietário não necessariamente possui direito de propriedade sobre o ativo, mas ele responde pelo mesmo junto aos demais colaboradores e aos gestores. Deve auxiliar, quando necessário, o proprietário do risco. O proprietário do ativo é designado durante a atividade de identificação de ativos.

Proprietário do risco de segurança da informação: pode ser o analista de risco, gestor de riscos ou qualquer outro colaborador. Tem a responsabilidade de gerenciar o risco que lhe foi designado e se reportar diretamente ao gestor de riscos. O proprietário do risco deve monitorar o risco sob sua tutela e assegurar que os controles estabelecidos por ele, com o auxílio do gestor e do analista de riscos, sejam de fato implementados. O proprietário do risco é designado durante a atividade de determinação de riscos.

Decisor sobre riscos de segurança da informação: é a presidência, direção ou o mais alto cargo da organização. Cabe a ele aprovar o plano de tratamento de riscos e decidir se aceita ou não os riscos residuais.

No decorrer do processo de gestão de riscos, ou após as iterações, poderá surgir a necessidade de definir novas funções ou redefinir os responsáveis por elas. É importante que essas alterações estejam sempre formalizadas para viabilizar a continuidade adequada e objetiva do processo.

4.2 Avaliação dos ativos de informação

Os ativos de informação consistem no cerne do processo de gestão de riscos da segurança da informação. Isso porque o objetivo imediato desse processo é garantir a segurança daqueles. Portanto, as atividades que envolvem a identificação e a valoração dos ativos correspondem a uma etapa única do processo destinada a avaliá-los. O produto final obtido nesta etapa é uma lista de ativos de informação com seus respectivos graus de criticidade para o negócio. Convém designar o proprietário para cada ativo. A avaliação da criticidade dos ativos é fundamental para a etapa seguinte, constituindo uma das variáveis para cálculo do risco.

4.2.1 Identificação dos ativos

Os ativos de informação que serão objeto da proteção no processo de gestão de riscos são aqueles que possuem valor para a organização. O valor do ativo não se restringe à quantia monetária que esse ativo representa ou ao seu custo de reposição. O ativo pode ser, por exemplo, os dados cadastrais de clientes, cuja divulgação não autorizada pode comprometer seriamente a credibilidade da organização.

Os ativos podem ser intangíveis, como fórmulas, processos, dados pessoais, dados financeiros; ou tangíveis, como mídias, computadores, substâncias, inventos, documentos em papel. Não raro, os ativos tangíveis tornam-se valiosos para a organização por servirem de suporte aos ativos intangíveis que de fato possuem valor e são o foco da gestão de riscos proposta nesta pesquisa.

Para a gestão de riscos, os ativos deverão ser listados, com os respectivos proprietários. Uma importante reflexão para escolha dos ativos que comporão a lista é avaliar se algum incidente de segurança que comprometa a confidencialidade, disponibilidade e/ou integridade do ativo trará prejuízos ao negócio da organização.

Sempre que o ativo intangível possuir um ativo tangível associado, como por exemplo, uma mídia removível que armazena os dados cadastrais dos clientes, esse ativo deverá ser identificado, pois pode ensejar novas variáveis que influenciarão a determinação do risco.

4.2.2 Valoração dos ativos

De posse da lista de ativos de informação, o próximo passo é avaliar o grau de criticidade de cada um, ou seja, avaliar quão importante é o ativo para o negócio da organização.

Como os ativos podem ser de difícil mensuração, sobretudo os intangíveis, optou-se por avaliá-los utilizando uma escala qualitativa (Quadro 2). A criticidade pode ser avaliada em baixa, média ou alta, com base na descrição definida para cada escala. Para atribuição da criticidade, não é necessário que o ativo corresponda a todos os aspectos apontados para cada valor qualitativo.

Quadro 2: Critérios para avaliação da criticidade

Criticidade	Definição
Alta	O ativo está diretamente relacionado à missão ou aos objetivos estratégicos e possui participação relevante no desempenho e lucratividade do negócio; possui alto custo e/ou tempo de reposição de forma que qualquer revés que venha a sofrer poderá afetar severamente o negócio da organização; está diretamente relacionado à segurança física das pessoas e do meio ambiente, de forma que um incidente com esse ativo pode resultar em danos severos à saúde das pessoas ou ao ambiente; ou o ativo está relacionado com dados que devem ser protegidos, como os casos previstos em lei, dados pessoais de clientes e colaboradores, e demais dados que a organização julgue ser necessário mantê-los sob sigilo.
Média	O ativo participa de atividades estratégicas relacionadas ao negócio, mas caso venha a sofrer alguma adversidade, trará prejuízos medianos à organização, sem afetar severamente o negócio; os custos de reposição são suportáveis e não causam endividamento significante ou não comprometem significativamente atividades estratégicas; não possui relação com a saúde e integridade das pessoas e pouco impacto tem sobre o meio ambiente.
Baixa	O ativo não possui relação com atividades estratégicas, de forma que qualquer dano que venha a sofrer poderá trazer impactos negativos em atividades administrativas ou de pouca relevância, sem causar prejuízos significantes ao negócio da empresa. Os custos de reposição são irrisórios se comparados ao orçamento e disponibilidade da organização.

Fonte - Produzido pelo autor do presente trabalho

A organização poderá definir critérios próprios para atribuição da criticidade para os ativos identificados.

4.3 Avaliação dos riscos

Nessa etapa são identificados e analisados os principais elementos que compõem o risco: ameaças, controles, vulnerabilidades, impacto e probabilidade. De posse desses dados, será possível calcular os riscos, que são o produto final da avaliação dos riscos. Poderão ser realizadas quantas iterações forem necessárias para avaliar adequadamente os riscos existentes e não omitir dados que possam influenciar na determinação desses riscos.

4.3.1 Identificação das ameaças

Ameaça é a possibilidade de ocorrência de um incidente que pode causar impactos negativos para a organização. Para que os riscos sejam adequadamente avaliados e tratados, torna-se necessário não apenas identificar as ameaças, mas também conhecer o seu perfil.

As ameaças podem ser internas ou externas à organização e podem ser classificadas segundo sua origem por: natural e humana (intencional e não-intencional). É importante conhecer o fator ou ator que dá origem a ameaça, denominado fonte da ameaça.

A identificação das ameaças deve envolver todos aqueles setores nos quais foram identificados ativos de informação. Os proprietários dos ativos podem fornecer dados importantes acerca de ameaças que podem afetar os ativos sob sua tutela. Ademais, existem catálogos, normas técnicas como a ISO 27005, publicações, especialistas, softwares, entre outros, que podem auxiliar na detecção de ameaças. Documentos e análises internas da organização, como o histórico de incidentes, também são úteis. O Nist sugere as fontes de ameaças mais comuns e agrupadas em quatro categorias, conforme quadro 3.

Quadro 3: Fontes de ameaças mais comuns

Tipo de fonte de ameaça	Descrição
INTENCIONAL • Individual: Externo, Interno, interno confiável, interno privilegiado. • Grupo: *ad hoc*, estabelecido. • Organização: concorrente, fornecedor, parceiro, cliente; • Nação-Estado.	Indivíduos, grupos, organizações ou Estados que buscam explorar a dependência da organização em recursos de informática (por exemplo, formulários eletrônicos e tecnologias de informação e comunicações).
ACIDENTAL • Usuário • Administrador/usuários privilegiado	Ações equivocadas executadas por indivíduos no curso de suas atividades rotineiras.
ESTRUTURAL • Equipamentos de Tecnologia da Informação: Armazenamento, Processamento, Comunicações, Visualização, Sensorial, Controlador. • Controles ambientais: Temperatura/umidade, Fornecimento de energia. • Software: Sistema Operacional, Rede, Aplicações de propósito geral, Aplicações de missão específica.	Falhas de equipamentos, controles ambientais ou em softwares devido ao envelhecimento, deterioração, desatualização e outras circunstâncias que excedem os parâmetros de operação.
AMBIENTAL • Natural ou ocasionada pelo homem: Fogo, enchente, alagamento, chuvas, tempestades, desmoronamentos, invasões. • Eventos naturais incomuns • Interrupção ou falha da infraestrutura: Telecomunicações, energia elétrica.	Desastres naturais e falhas em infraestruturas críticas das quais a organização depende, mas que fogem ao seu controle.

Fonte - Traduzido e adaptado de Nist (2011, p. D-2)

As ameaças podem afetar mais de um ativo, hipótese da qual resultarão cenários distintos e, portanto, riscos distintos.

4.3.2 Identificação e avaliação dos controles

Controle diz respeito à medida de segurança proposta ou implementada para evitar incidentes que possam comprometer a disponibilidade, integridade e confidencialidade de um determinado ativo. Em geral, as organizações já dispõem de controles implementados mesmo antes de iniciar a gestão de riscos de segurança da informação.

Nessa etapa, deverão ser identificados todos os controles já implementados com os respectivos ativos a que visam proteger. Em seguida, procede-se à avaliação desses controles, com o objetivo de verificar se estão adequados para o fim a que se propõem. Os controles que forem avaliados como insatisfatórios devem ser especificados com as respectivas justificativas para essa avaliação. Controles insatisfatórios ensejam vulnerabilidades, que serão objeto de análise da atividade seguinte.

Os controles implementados com base no plano de tratamento de riscos, elaborado nas etapas finais do processo, serão avaliados à medida que novas iterações da gestão de riscos forem realizadas.

Para cada controle identificado deverá ser atribuída uma das duas qualificações descritas na quadro 4.

Quadro 4: Referência para avaliação de controles

Avaliação do controle	**Critérios**
Insatisfatório	O controle apresenta falhas técnicas, humanas, processuais ou operacionais que o tornam ineficaz, não assegurando de forma adequada a disponibilidade, integridade e/ou confidencialidade do ativo que visa a proteger.
Satisfatório	O controle é eficaz e cumpre adequadamente o objetivo para o qual foi implementado, qual seja o de garantir a disponibilidade, integridade e/ou confidencialidade do ativo.

Fonte –Produzido pelo autor do presente trabalho

4.3.3 Identificação das vulnerabilidades

Vulnerabilidade é uma fraqueza ou falha do ativo de informação que pode ser explorada por uma ameaça. Para efeito de gestão de riscos, as vulnerabilidades

e ameaças são analisadas aos pares, de forma que somente serão consideradas as vulnerabilidades que podem de fato ser exploradas por uma ameaça.

Os controles considerados insatisfatórios deverão ser considerados para identificação das vulnerabilidades. Ademais, os ativos deverão ser analisados, um a um, com o objetivo de identificar outros aspectos, os quais podem estar ligados a propriedades do ativo, que possam constituir uma vulnerabilidade a ser explorada por uma ameaça.

Convém utilizar softwares especializados para identificação de vulnerabilidade técnicas relacionadas à tecnologia da informação.

4.3.4 Avaliação do Impacto

Para fins da gestão de riscos, impacto refere-se ao resultado negativo de um incidente de segurança. Para avaliar o impacto, em primeiro lugar, é necessário elaborar uma lista de cenários, combinando as informações dos ativos, ameaças e vulnerabilidades levantadas nas etapas anteriores, e estimando os impactos resultantes da exploração de vulnerabilidade por uma ameaça, conforme quadro 5.

Quadro 5: Exemplo de cenário de incidente de segurança com o impacto

Ativo	Ativo associado	Ameaça	Vulnerabilidade	Cenário com impacto
Dados de fornecedores	Sistema de cadastro	Acesso/alteração de dados não autorizado (a)	Ausência de autenticação para acesso ao sistema	Acesso indevido, por indivíduo não autorizado, ao sistema de cadastro, apagando os dados de fornecedores

Fonte –Produzido pelo autor do presente trabalho

Para cada trio ativo-ameaça-vulnerabilidade deverá ser elaborado um cenário de incidente de segurança, com o respectivo impacto, pois gera um risco específico. Em seguida, o impacto descrito em cada cenário será avaliado, com base na quadro 6, traduzida e adaptada do Nist (2011, p. H-3):

Quadro 6: Avaliação do impacto

Avaliação do Impacto	Descrição
Alto	O incidente de segurança pode causar efeitos severos ou catastróficos nas operações, processos, ativos, indivíduos, e outras organizações. Esses efeitos inviabilizam severamente a missão e/ou os objetivos estratégicos ou ainda causam prejuízos exorbitantes às finanças e/ou imagem da organização.
Médio	O incidente de segurança pode causar efeitos sérios nas operações, processos, ativos, indivíduos, e outras organizações. Esses efeitos prejudicam significativamente a missão e/ou os objetivos estratégicos ou ainda causam prejuízos consideráveis às finanças e/ou imagem da organização.
Baixo	O incidente de segurança pode causar efeitos limitados nas operações, processos, ativos, indivíduos, e outras organizações. Esses efeitos não comprometem a missão e/ou os objetivos estratégicos e os prejuízos resultantes são facilmente reversíveis.

Fonte – Traduzido e adaptado de Nist (2011, p. H-3)

Os valores qualitativos atribuídos para cada cenário serão considerados para efeito de cálculo do risco.

4.3.5 Avaliação da probabilidade

A probabilidade consiste na chance de alguma ameaça explorar uma vulnerabilidade, associada a um ativo, gerando prejuízos à organização. A avaliação da probabilidade envolve a análise dos cenários de incidentes de segurança, elaborados na atividade anterior.

Para o presente modelo a probabilidade não consiste em um valor matemático, mas em um valor qualitativo, conforme o quadro 7.

Quadro 7: Avaliação da probabilidade de incidentes de segurança

Avaliação da Probabilidade	Descrição
Alta	Há forte possibilidade de que o incidente aconteça, o que pode ser corroborado pelo histórico frequente de ocorrência desse tipo de incidente. A fonte da ameaça mostra-se decidida em explorar alguma vulnerabilidade.

Média	O incidente pode ocorrer eventualmente, como já ocorreu algumas vezes na organização. A fonte da ameaça pode explorar a vulnerabilidade a depender das circunstâncias que venham lhe favorecer.
Baixa	A ocorrência do incidente é improvável, podendo dar-se em circunstâncias excepcionais. Apesar de existir uma ameaça capaz de provocar o incidente, a fonte de ameaça pouco interesse ou capacidade tem para iniciar o evento.

Fonte - Produzido pelo autor do presente trabalho

O produto final dessa etapa é uma lista com todos os cenários de incidentes de segurança, avaliados segundo sua probabilidade de ocorrência.

4.3.6 Determinação dos riscos

O risco, para o presente modelo de gestão de riscos, consiste em um valor qualitativo dado a um cenário de incidente de segurança, resultado da combinação da (i) criticidade do ativo, (ii) probabilidade de que uma ameaça possa explorar alguma vulnerabilidade de um ativo, e o (iii) impacto que esse evento trará para a organização.

Nessa etapa, o risco é calculado utilizando-se uma análise qualitativa, conforme quadro 8. O risco é determinado por meio do cruzamento dos valores das três variáveis (criticidade, probabilidade e impacto), podendo assumir os valores baixo, médio ou alto. A matriz para determinação de riscos poderá ser alterada conforme as especificidades de cada organização e o peso que se deseja atribuir a cada variável, para fins de cálculo do risco. No quadro 8, maior peso foi dado à variável impacto, de forma que sempre que um cenário apresentar alto impacto, média ou alta probabilidade, independente da criticidade do ativo, será considerado de alto risco.

Quadro 8: Matriz para determinação de riscos

Determinação do risco				
Probabilidade	**Criticidade**	**Impacto**		
		Baixo	**Médio**	**Alto**
Baixa	**Baixa**	**Baixo**	**Baixo**	**Médio**
	Média	**Baixo**	**Baixo**	**Médio**
	Alta	**Baixo**	**Médio**	**Médio**
Média	**Baixa**	**Baixo**	**Médio**	**Alto**
	Média	**Baixo**	**Médio**	**Alto**
	Alta	**Médio**	**Médio**	**Alto**
Alta	**Baixa**	**Médio**	**Médio**	**Alto**
	Média	**Médio**	**Alto**	**Alto**
	Alta	**Alto**	**Alto**	**Alto**

Fonte - Produzido pelo autor do presente trabalho

Após a consolidação de uma lista dos cenários de incidentes de segurança com os respectivos níveis de risco, deve-se indicar um responsável por monitorar o risco e assegurar a implementação das ações traçadas para reduzi-lo, definidas na etapa posterior. Convém que os cenários sejam organizados por ordem do maior para menor nível de risco, para facilitar sua priorização na etapa de tratamento de riscos.

Para as organizações que implementarem a gestão de riscos pela primeira vez, é possível que cheguem a uma extensa lista de cenários com riscos. Contudo, à medida que esses riscos forem tratados em iterações sucessivas, a tendência é de que essa lista seja reduzida.

4.4 Tratamento dos riscos

O tratamento do risco consiste na solução para reduzir o risco ao menor nível possível. A solução pode ser por meio da implementação ou alteração de controles (medidas de segurança) ou por meio da alteração de algum fator (ameaça, vulnerabilidade, impacto, probabilidade) que possa reduzir o nível de risco.

4.4.1 Plano de tratamento dos riscos

O primeiro passo para o tratamento de riscos é analisar a avaliação dos controles, realizada em etapa anterior do processo de gestão de riscos, com o objetivo de propor melhorias ou exclusão dos controles considerados insatisfatórios. Em seguida, deverão ser propostos controles adicionais, tomando como base a lista de vulnerabilidades encontradas, para assegurar a proteção dos ativos contra as ameaças identificadas. Por fim, a lista de cenários também será útil para vislumbrar soluções que não estejam diretamente ligadas a uma medida de segurança, mas que poderão reduzir o impacto ou a probabilidade de um incidente de segurança, reduzindo, por conseguinte, o nível do risco.

O produto desta etapa consiste em um plano de tratamento de riscos, com o detalhamento das soluções encontradas para reduzir cada risco.

4.4.2 Determinação dos riscos residuais

Risco residual é o risco remanescente após o tratamento. Para determiná-lo, é necessário realizar nova avaliação dos riscos, levando em consideração os efeitos previstos com a implementação do plano de tratamento de riscos. Qualquer alteração em uma das três variáveis que compõem o cálculo do risco (criticidade, impacto e probabilidade), deverá alterar também o nível do risco.

O resultado dessa atividade é uma lista com todos os riscos identificados, o plano de tratamento, e os riscos residuais.

4.5 Decisão sobre os riscos

A tolerância em relação aos riscos varia de acordo com o perfil da organização e com as percepções acerca da segurança da informação. Em organizações menos tolerantes aos riscos, os gestores poderão considerar níveis médios inaceitáveis e tomarão as medidas necessárias, mesmo que sejam mais onerosas, para reduzir os riscos ao nível baixo. Já organizações mais tolerantes poderão suportar níveis mais altos dos riscos.

A tolerância ao risco, portanto, deverá ser determinada pelos gestores, diretores ou presidentes da organização, os quais possuem a responsabilidade e autoridade necessárias para assumir as consequências decorrentes da decisão sobre os riscos. Cabe-lhes analisar criticamente os riscos identificados, o plano de tratamento, e os riscos residuais, levando em consideração o custo/benefício da solução prevista no plano de tratamento e os efeitos desejáveis.

A análise pela alta gestão deverá apontar:

- As soluções consideradas inviáveis ou inaceitáveis;
- Soluções que por ventura não tenham sido consideradas nas etapas anteriores;
- Modificação em soluções apontadas;
- Riscos altos que estejam dispostos a assumir, mesmo após o tratamento, com a devida justificativa;
- Riscos que desejam compartilhar com outras organizações;
- Riscos residuais inaceitáveis;
- Outras observações que julgar necessárias referentes à segurança da informação.

Após análise crítica dos riscos e do plano de tratamento, uma nova avaliação dos riscos poderá ser necessária a depender dos apontamentos realizados pela alta gestão. Ao final, a análise retorna à alta gestão para aprovação, após a qual o plano de tratamento deverá ser implementado.

É importante que os atores envolvidos na gestão dos riscos acompanhem a implementação do plano de tratamento, mesmo que as soluções não estejam diretamente relacionadas à sua área de atuação.

4.6 Monitoramento e comunicação

O processo de gestão de riscos é dinâmico e deve considerar imediatamente qualquer mudança no ambiente da organização que possa afetar os riscos à segurança da informação. Isso torna necessário o monitoramento contínuo do contexto interno e externo da organização, dos fatores do risco (ativos, ameaças,

vulnerabilidades, impacto, probabilidades), e do tratamento dos riscos, a fim de permitir a adequada avaliação dos riscos e a implementação oportuna de soluções de segurança.

Para que o monitoramento seja efetivo, convém estabelecer um plano de comunicação que defina como se dará a interação entre os principais atores do processo de gestão de riscos, otimizando a coleta, registro e difusão de informações acerca dos riscos à segurança da informação. O plano de comunicação deve permitir que a alta gestão esteja permanentemente informada acerca de todo o processo de gestão de riscos.

5 DEMONSTRAÇÃO DO MODELO DE GESTÃO DE RISCOS

O modelo de gestão de riscos de segurança da informação será demonstrado, em estudo de caso, por meio de sua aplicação em uma instituição de ensino fictícia aqui denominada Educação Inovadora.

O processo de gestão de riscos será demonstrado em apenas uma iteração e até a etapa do tratamento de riscos. As etapas bem como as atividades a serem realizadas na demonstração da aplicação do modelo constam na figura 7.

Figura 7: Atividades a serem realizadas na demonstração da aplicação do modelo

Fonte – Produzido pelo autor do presente trabalho

A etapa da decisão sobre os riscos, prevista no modelo, torna-se desnecessária para fins de demonstração, devido ao caráter subjetivo dessa atividade.

As atividades que envolvem julgamentos segundo critérios qualitativos (valoração dos ativos, avaliação dos controles, avaliação do impacto e avaliação da probabilidade), tomarão como base os dados levantados sobre a organização na

primeira etapa (planejamento da gestão de riscos), que envolve a definição de contexto e a definição de papéis e responsabilidades.

A atividade de definição do contexto da Educação Inovadora (organização fictícia) terá como principal referência a escola na qual o autor concluiu o ensino médio, em Brasília, e cuja divulgação do nome não foi autorizada. Também serão utilizados dados disponíveis na internet sobre outras escolas de Brasília.

Algumas atividades serão agrupadas em uma mesma seção com o intuito de facilitar a visualização do encadeamento lógico das fases previstas no modelo de gestão de riscos da segurança da informação.

5.1 Planejamento da gestão de riscos

A etapa do planejamento envolve a definição do contexto e o estabelecimento dos papéis e responsabilidades.

5.1.1 Definição do Contexto

A instituição denomina-se Educação Inovadora e está sediada em Brasília/DF. Não dispõe de filiais. Oferece serviços privados de educação do ensino básico (Ensino Infantil e Fundamental). Possui 60 funcionários, das mais diversas formações, e 1200 alunos matriculados no ano de 2014.

Negócio: ensino básico (infantil e fundamental).

Visão: ser referencial de uma educação de excelência e inovadora.

Missão: proporcionar uma educação de excelência para crianças e adolescentes, promovendo a formação humana e a cultura da solidariedade.

Valores: ética, excelência, solidariedade e inovação.

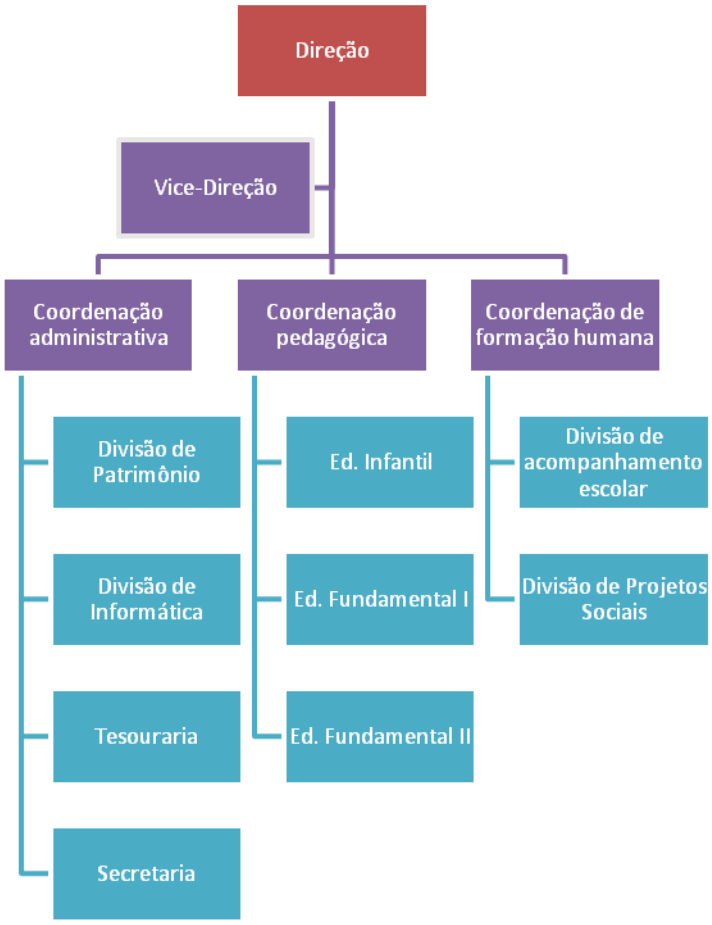
Objetivos estratégicos:

- Aumentar em 5%, até 2015, o rendimento escolar global da escola;
- Alcançar, até 2020, 2000 matrículas;

- Aumentar o número de renovações de matrículas em pelo menos 5% até 2016;
- Garantir 90% de satisfação em pesquisa anual aplicada às famílias com relação à escola;
- Reforçar e ampliar os projetos sociais desenvolvidos pela escola com o apoio dos alunos.

Organograma:

Figura 6: Organograma da Instituição Educação Inovadora



Fonte - Produzido pelo autor do presente trabalho

A estrutura da instituição é hierárquica de forma que somente os coordenadores possuem acesso direto à direção e vice-direção. Cada seção possui uma chefia que responde a chefia imediatamente superior. As coordenações intermediam a troca de informações entre as seções sob sua responsabilidade.

A divisão de informática é responsável pelos equipamentos e recursos que digam respeito à tecnologia da informação. A divisão possui apenas dois funcionários que ficam lotados no laboratório de informática, que é regularmente utilizado para atividades pedagógicas com os alunos. Não há uma função relacionada à segurança da informação. As soluções de segurança são aplicadas conforme necessidade.

Localidade e características geográficas: A instituição está sediada na 902 norte, Brasília/DF, em uma área de 10mil m2. O terreno situado nas imediações do perímetro da escola é baldio e atualmente está com a vegetação alta. Há uma delegacia de polícia civil a cerca de 200m e um shopping situado a 1 km. O trânsito das imediações é relativamente tranquilo, à exceção do período de 7h às 7h30 e 12h às 12h30, horário de entrada e saída de alunos respectivamente.

Aspectos legais e contratuais: a instituição se sujeita às exigências do Ministério da Educação no que concerne o currículo pedagógico, à Lei de Diretrizes e Bases da Educação Nacional e ao Estatuto da Criança e do Adolescente. Deve obedecer ainda ao regimento interno.

Segurança da Informação: a Educação Inovadora não dispõe da Política de Segurança da Informação. Em geral, os gestores percebem a importância da segurança da informação, mas desconhecem as medidas necessárias para implementar a gestão de riscos. Recentemente, a instituição sofreu um ataque cibernético que resultou na suspensão do serviço de pagamentos da escola por dois dias. O backup disponível não estava atualizado e por essa razão alguns dados financeiros foram perdidos. Os gestores pretendem resguardar-se contra ataques como esses e proteger os dados tanto da instituição como de seus clientes.

Expectativas das partes interessadas: Alguns fornecedores de serviços como água, luz, alimentos e manutenções prediais podem ser prejudicados caso a instituição seja impossibilitada de honrar seus compromissos financeiros, em decorrência de alguma falha na segurança da informação. Os gestores exigem o correto funcionamento do sistema de gestão de patrimônio e de pagamento de funcionários. Os clientes esperam que suas informações pessoais sejam protegidas contra a divulgação não autorizada pela escola.

Restrições: a instituição dispõe de orçamento limitado e a divisão de informática conta com número excessivamente reduzido de funcionários que se dedicam predominantemente às atividades de suporte a usuário. Ademais, não possuem formação e experiência com segurança da informação.

Objetivo da gestão de riscos: A gestão de riscos deverá ser aplicada em toda a escola, devendo considerar todas as informações de valor para a instituição. A gestão de riscos deverá fazer parte, de forma contínua e sistemática, das atividades da Divisão de Informática, que passará a ter acesso direto à direção.

5.1.2 Papéis e responsabilidades

Gestor de riscos de segurança da informação: Chefe da Divisão de Informática. Será responsável por assegurar o correto andamento de todas as fases do processo de gestão de riscos. Deverá manter a direção informada acerca do processo.

Analista de riscos de segurança da informação: Colaborador lotado na Divisão de Informática. Deverá proceder à execução operacional das atividades previstas no processo.

Decisor sobre riscos de segurança da informação: diretor e vice-diretor. Tomarão as decisões sobre os riscos residuais e deverão apreciar e aprovar o plano de tratamento de riscos.

Colaboradores de outras seções poderão ser convocados para atuar nas demais fases do processo de gestão de riscos.

5.2 Avaliação dos ativos de informação

A etapa da avaliação dos ativos envolve as atividades de identificação e valoração desses.

5.2.1 Identificação e valoração dos ativos

Os ativos foram identificados e valorados conforme Quadro 9. A valoração toma como base os critérios sugeridos no modelo.

Quadro 9: Identificação e valoração dos ativos da Educação Inovadora

Ativo	Ativo associado	Objetivo de segurança	Proprietário do ativo	Criticidade
Dados pessoais sobre os clientes (pais e alunos)	Arquivo físico; sistema de cadastro; servidor de armazenamento de arquivos.	Confidencialidade, disponibilidade e integridade.	Administrador do sistema de cadastro	**Alta**
Dados financeiros da instituição	Sistema de pagamento de funcionários e fornecedores, arquivo físico.	Confidencialidade, disponibilidade e integridade.	Coordenador de administração	**Média**
Dados sobre desempenho pedagógico e menções de alunos	Arquivo físico; servidor de armazenamento de arquivos.	Disponibilidade e integridade	Coordenadora pedagógica	**Alta**
Provas a serem realizadas	Arquivo físico; servidor de armazenamento de arquivos.	Confidencialidade	Coordenadora pedagógica	**Média**
Projetos sociais	Arquivo físico; servidor de armazenamento de arquivos.	Disponibilidade e integridade	Chefe da Divisão de Projetos Sociais	**Baixa**
Sistema de pagamento de funcionários e fornecedores	-	Confidencialidade, disponibilidade e integridade.	Administrador do sistema de pagamento de funcionários e fornecedores	**Alta**

Fonte – Produzido pelo autor do presente trabalho

5.3 Avaliação dos riscos

Na etapa de avaliação dos riscos, são realizadas as atividades de identificação de ameaças, identificação e avaliação dos controles, identificação de vulnerabilidades, avaliação de impacto, avaliação da probabilidade e determinação do risco.

5.3.1 Identificação das ameaças, identificação e avaliação dos controles e identificação das vulnerabilidades.

As ameaças, vulnerabilidades e controles identificados, bem como a avaliação dos últimos constam no Quadro 10.

Quadro 10: Ameaças, controles e vulnerabilidades da Educação Inovadora

Ativo	Ativos associado	Ameaça	Controle	Avaliação do controle	Vulnerabilidade
Dados pessoais sobre os clientes (pais e alunos)	Arquivo físico; sistema de cadastro; servidor de armazenamento de arquivos	Fogo, Inundação, Interrupção do serviço de energia, furto de equipamentos e documentos, divulgação e/ou alteração indevida, falha de sistema.	Senha para acesso ao servidor de arquivos	Insatisfatório	Não há gerador de energia. Não há política para troca regular de senhas. O tráfego e sistemas da rede local não são criptografados. Não há política de *backup* do sistema. Não há sistema de escoamento de água pluvial.
			Extintor na sala do servidor de arquivos	Satisfatório	
			Acesso restrito e autenticação do usuário para o sistema de cadastro	Insatisfatório	
			Alarme no perímetro da escola interligado à central de segurança	Satisfatório	
Dados financeiros da instituição	Sistema de pagamento de funcionários e fornecedores.	Falha do sistema, divulgação e/ou alteração indevida.	Há backup do sistema.	Insatisfatório	Não há política para troca regular de senhas. O tráfego e sistemas da rede local não são criptografados. Não há política de *backup* regular do sistema.
			Senha para acesso ao sistema	Insatisfatório	
Dados sobre desempenho	Arquivo físico; servidor de	Fogo, Inundação, Interrupção do serviço	Senha para acesso ao servidor de arquivos	Insatisfatório	Não há gerador de energia. Não há política para troca regular de

pedagógico e menções de alunos	armazenamento de arquivos	de energia, furto de equipamentos e documentos, alteração indevida/perda de dados.	Extintor na sala do servidor de arquivos	Satisfatório	senhas. O tráfego e sistemas da rede local não são criptografados. Não há política de *backup* do servidor. Não há sistema de escoamento de água pluvial. Possibilidade acesso de alunos a computadores com dados sobre as menções.
			Alarme no perímetro da escola interligado à central de segurança	Satisfatório	
Provas a serem realizadas	Arquivo físico; servidor de armazenamento de arquivos	Fogo, Inundação, Interrupção do serviço de energia, furto de equipamentos e documentos, acesso e alteração indevida.	Senha para acesso ao servidor de arquivos	Insatisfatório	Não há gerador de energia. Não há política para troca regular de senhas. Não há política de *backup* do servidor. Não há sistema de escoamento de água pluvial. Possibilidade de acesso de alunos a computadores com menções.
			Extintor na sala do servidor de arquivos	Satisfatório	
			Alarme no perímetro da escola interligado à central de segurança	Satisfatório	
Projetos sociais	Arquivo físico; servidor de armazenamento de arquivos	Fogo, Inundação, Interrupção do serviço de energia, furto de equipamentos e documentos, alteração de dados/perda de dados	Senha para acesso ao servidor de arquivos	Insatisfatório	Não há gerador de energia. Não há política para troca regular de senhas. O tráfego e sistemas da rede local não são criptografados. Não há política de *backup* do servidor. Não há sistema de escoamento de água pluvial.
			Extintor na sala do servidor de arquivos	Satisfatório	
			Alarme no perímetro da escola interligado à central de segurança	Satisfatório	
Sistema de pagamento de funcionários e fornecedores	-	Falha do sistema, divulgação e/ou alteração indevida.	Senha para acesso ao sistema	Insatisfatório	Não há política para troca regular de senhas. O tráfego da rede local e dos sistemas não é criptografado. O firewall não dispõe de IPS e IDS.
			Firewall para controle de acesso à rede	Insatisfatório	

Fonte: Produzido pelo autor do presente trabalho

5.3.2 Avaliação do impacto, avaliação da probabilidade e determinação dos riscos

Para cada trio ativo-ameaça-vulnerabilidade, foram elaborados cenários de incidentes. Com os níveis apontados para as três variáveis impacto, probabilidade, criticidade, utilizando os critérios constantes, respectivamente, dos Quadros 6, 7 e 2, foram determinados os riscos para cada cenário, conforme matriz sugerida no modelo (Quadro 8). Os dados sobre os riscos constam no Quadro 11.

Quadro 11: Impacto, probabilidade e riscos da Educação Inovadora

Ativo	Ameaça	Vulnerabilidade	Cenário de incidente	Impacto	Probabilidade	Criticidade	Risco
Dados pessoais sobre os clientes (pais e alunos)	Interrupção de energia	Não há gerador de energia	Comprometimento dos dados pessoais dos clientes devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Baixo**	**Alta**[1]	**Alta**	**Alto**
	Inundação	Não há sistema de escoamento de águas pluviais	Comprometimento dos dados pessoais dos clientes devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Baixo**	**Alta**[2]	**Alta**	**Alto**
	Divulgação/ alteração indevida	Não há política para troca regular de senhas.	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixa**	**Alta**	**Baixo**
		O tráfego e sistemas da rede local não são criptografados	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido à invasão e captura de dados por hacker.	**Baixo**	**Baixa**	**Alta**	**Baixo**
	Falha de	Não há política de	Comprometimento dos dados pessoais	**Baixo**	**Média**	**Alta**	**Médio**

[1] A probabilidade de comprometimento dos dados pessoais dos clientes devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado é alta, pois a rede de energia elétrica da região é instável, o que resultado em interrupções frequentes do fornecimento de energia para a Escola. Trata-se de uma situação fictícia que exemplifica a a avaliação da probabilidade conforme os critérios definidos no modelo proposto.

[2] A probabilidade de comprometimento dos dados pessoais dos clientes devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações é alta, pois sempre que ocorrem chuvas com fortes ventos, inundam-se as instalações subterrâneas da Escola, local em que se situa o servidor de arquivos. Trata-se de uma situação fictícia que exemplifica a a avaliação da probabilidade conforme os critérios definidos no modelo proposto.

	sistema	*backup* do sistema	dos clientes devido à falha do sistema e ausência de *backup* atualizado.				
Dados financeiros da instituição	Falha do sistema	Não há política de *backup* regular do sistema.	Comprometimento dos dados financeiros devido a falha do sistema de pagamentos de funcionários e fornecedores e à ausência de *backup* atualizado.	**Médio**	**Média**	**Média**	**Médio**
	Divulgação e/ou alteração indevida.	O tráfego e sistemas da rede local não são criptografados.	Divulgação e/ou alteração indevida dos dados financeiros da instituição devido à invasão e captura de dados por hacker.	**Médio**	**Média**	**Média**	**Médio**
	Divulgação e/ou alteração indevida.	Não há política para troca regular de senhas.	Divulgação e/ou alteração indevida dos dados financeiros da instituição devido ao acesso não-autorizado por meio de senha de usuário.	**Médio**	**Baixa**	**Média**	**Baixo**
Dados sobre desempenho pedagógico e menções de alunos	Interrupção do serviço de energia	Não há gerador de energia.	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Médio**	**Alta**	**Alta**	**Alto**
	Inundação	Não há sistema de escoamento de água pluvial.	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Médio**	**Alta**	**Alta**	**Alto**
	Alteração de dados/perda de dados	Não há política de *backup* do servidor.	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido a falhas técnicas no servidor de arquivos e ausência de *backup* atualizado.	**Baixo**	**Média**	**Alta**	**Médio**
		Possibilidade de acesso de alunos a computadores com	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à ação de	**Baixo**	**Média**	**Alta**	**Médio**

		menções.	alunos mal intencionados com acesso a computadores com as menções.				
		Não há política para troca regular de senhas.	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixa**	**Alta**	**Baixo**
		O tráfego e sistemas da rede local não são criptografados	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à invasão e captura de dados por hacker.	**Baixo**	**Baixa**	**Alta**	**Baixo**
Provas a serem realizadas	Inundação	Não há sistema de escoamento de água pluvial.	Comprometimento das provas a serem realizadas devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Baixo**	**Alta**	**Média**	**Médio**
	Interrupção do serviço de energia	Não há gerador de energia.	Comprometimento das provas a serem realizadas devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Baixo**	**Alta**	**Média**	**Médio**
	Acesso e alteração indevida de dados	Não há política para troca regular de senhas.	Acesso e alteração indevida de dados das provas a serem realizadas devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Média**	**Média**	**Baixo**
		Possibilidade de acesso de alunos a computadores com menções.	Acesso e alteração indevida de dados das provas a serem realizadas devido à ação de alunos mal intencionados com acesso a computadores com as menções.	**Baixo**	**Média**	**Média**	**Baixo**
Projetos sociais	Inundação	Não há sistema de escoamento de água pluvial.	Comprometimento dos dados de projetos sociais devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Baixo**	**Alta**	**Baixa**	**Médio**

	Interrupção do serviço de energia	Não há gerador de energia.	Comprometimento dos dados de projetos sociais devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Baixo**	**Alta**	**Baixa**	**Médio**
	Alteração de dados/perda de dados	Não há política de *backup* do servidor.	Perda dos dados sobre projetos sociais devido à ausência de *backup* atualizado.	**Baixo**	**Média**	**Baixa**	**Baixo**
	Alteração de dados/perda de dados	Não há política para troca regular de senhas.	Alteração/perda de dados sobre os projetos sociais devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixa**	**Baixa**	**Baixo**
Sistema de pagamento de funcionários e fornecedores	Divulgação e/ou alteração indevida.	Não há política para troca regular de senhas.	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido ao acesso não-autorizado por meio de senha de usuário.	**Médio**	**Baixa**	**Alta**	**Médio**
	Divulgação e/ou alteração indevida.	O tráfego da rede local e dos sistemas não é criptografado.	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão e captura de dados por hacker.	**Médio**	**Média**	**Alta**	**Médio**
	Divulgação e/ou alteração indevida.	O firewall não dispõe de IPS e IDS.	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão pelo firewall e captura de dados por hacker.	**Médio**	**Média**	**Alta**	**Médio**

Fonte: Produzido pelo autor do presente trabalho

Tendo em vista o efetivo reduzido da escola para o setor de informática/segurança, o chefe da divisão de informática assumirá a propriedade de todos os riscos identificados.

5.3.3 Priorização dos riscos

Como sugere o modelo de gestão de riscos, os riscos identificados na Educação Inovadora foram ordenados por ordem decrescente de nível no Quadro 12, com o intuito de facilitar a visualização dos riscos e priorizar o tratamento daqueles considerados mais altos.

Quadro 12: Priorização dos riscos da Educação Inovadora

Nº	Cenário	Risco
01	Comprometimento dos dados pessoais dos clientes devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Alto**
02	Comprometimento dos dados pessoais dos clientes devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Alto**
03	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Alto**
04	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Alto**
05	Comprometimento dos dados pessoais dos clientes devido à falha do sistema e ausência de *backup* atualizado.	**Médio**
06	Comprometimento dos dados financeiros devido à falha do sistema de pagamentos de funcionários e fornecedores e à ausência de *backup* atualizado.	**Médio**
07	Divulgação e/ou alteração indevida dos dados financeiros da instituição devido à invasão e captura de dados por hacker.	**Médio**
08	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido a falhas técnicas no servidor de arquivos e ausência de *backup* atualizado.	**Médio**
09	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à ação de alunos mal intencionados com acesso a computadores com as menções.	**Médio**
10	Comprometimento das provas a serem realizadas devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Médio**
11	Comprometimento das provas a serem realizadas devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Médio**
12	Comprometimento dos dados de projetos sociais devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Médio**

13	Comprometimento dos dados de projetos sociais devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Médio**
14	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido ao acesso não-autorizado por meio de senha de usuário.	**Médio**
15	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão e captura de dados por hacker.	**Médio**
16	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão do firewall e captura de dados por hacker.	**Médio**
17	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**
18	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido à invasão e captura de dados por hacker.	**Baixo**
19	Divulgação e/ou alteração indevida dos dados financeiros da instituição devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**
20	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**
21	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à invasão e captura de dados por hacker.	**Baixo**
22	Acesso e alteração indevida de dados das provas a serem realizadas devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**
23	Acesso e alteração indevida de dados das provas a serem realizadas devido à ação de alunos mal intencionados com acesso a computadores com as menções.	**Baixo**
24	Perda dos dados sobre projetos sociais devido à ausência de *backup* atualizado.	**Baixo**
25	Alteração/perda de dados sobre os projetos sociais devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**

Fonte: Produzido pelo autor do presente trabalho

5.4 Tratamento dos riscos

A etapa do tratamento de riscos envolve a elaboração de um plano de tratamento de riscos e da determinação dos níveis residuais, considerando os efeitos previstos da implementação do plano.

5.4.1 Plano de tratamento dos riscos

Para cada cenário de incidente, foram sugeridas soluções que possam mitigar o nível do risco. As soluções propostas constam no Plano de tratamento de riscos, definido no Quadro 13.

Quadro 13: Plano de tratamento de riscos da Educação Inovadora

Nº	Cenário	Solução
1	Comprometimento dos dados pessoais dos clientes devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	Instalar gerador de energia elétrica com autonomia de pelo menos 2 horas. Custo: 50 mil reais.
2	Comprometimento dos dados pessoais dos clientes devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	Instalação de sistema de escoamento de águas pluviais nas imediações prediais. Custo: 100 mil reais.
3	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	Instalar gerador de energia elétrica com autonomia de pelo menos 2 horas. Custo: 50 mil reais.
4	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	Instalação de sistema de escoamento de águas pluviais nas imediações prediais. Custo: 100 mil reais.
5	Comprometimento dos dados pessoais dos clientes devido à falha do sistema e ausência de *backup* atualizado.	Instituir política de *backup* prevendo como, quem, e com que frequência será realizado o *backup*. Custo: zero.
6	Comprometimento dos dados financeiros devido à falha do sistema de pagamentos de funcionários e fornecedores e à ausência de *backup* atualizado.	Instituir política de *backup* prevendo como, quem, e com que frequência será realizado o *backup*. Custo: zero.
7	Divulgação e/ou alteração indevida dos dados financeiros da instituição devido à invasão e captura de dados por hacker.	Criptografar o tráfego da rede local bem como os dados armazenados no servidor. Custo: zero.
8	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido a falhas técnicas e ausência de *backup* atualizado.	Instituir política de *backup* prevendo como, quem, e com que frequência será realizado o *backup*. Custo: zero.

9	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à ação de alunos mal intencionados com acesso a computadores com as menções.	Limitar o acesso físico e lógico de alunos aos computadores com as menções. Custo: 2000 reais.
10	Comprometimento das provas a serem realizadas devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	Instalação de sistema de escoamento de águas pluviais nas imediações prediais. Custo: 100 mil reais.
11	Comprometimento das provas a serem realizadas devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	Instalar gerador de energia elétrica com autonomia de pelo menos 2 horas. Custo: 50 mil reais.
12	Comprometimento dos dados de projetos sociais devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	Instalação de sistema de escoamento de águas pluviais nas imediações prediais. Custo: 100 mil reais.
13	Comprometimento dos dados de projetos sociais devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	Instalar gerador de energia elétrica com autonomia de pelo menos 2 horas. Custo: 50 mil reais.
14	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido ao acesso não-autorizado por meio de senha de usuário.	Instituir política de senhas, definindo padrões seguros de senhas (alfanuméricos com mais de 12 caracteres) e curta periodicidade para troca de senhas. Custo: zero.
15	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão e captura de dados por hacker.	Criptografar o tráfego da rede local bem como os dados armazenados no servidor. Custo: zero.
16	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão do firewall e captura de dados por hacker.	Contratar as funcionalidades de IPS e IDS para o firewall. Custo: 20mil reais.
17	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido ao acesso não-autorizado por meio de senha de usuário.	Instituir política de senhas, definindo padrões seguros de senhas (alfanuméricos com mais de 12 caracteres) e curta periodicidade para troca de senhas. Custo: zero.
18	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido à invasão e captura de dados por hacker.	Criptografar o tráfego da rede local bem como os dados armazenados no servidor. Custo: zero.
19	Divulgação e/ou alteração indevida dos dados	Instituir política de senhas,

	financeiros da instituição devido ao acesso não-autorizado por meio de senha de usuário.	definindo padrões seguros de senhas (alfanuméricos com mais de 12 caracteres) e curta periodicidade para troca de senhas. Custo: zero.
20	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido ao acesso não-autorizado por meio de senha de usuário.	Instituir política de senhas, definindo padrões seguros de senhas (alfanuméricos com mais de 12 caracteres) e curta periodicidade para troca de senhas. Custo: zero.
21	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à invasão e captura de dados por hacker.	Criptografar o tráfego da rede local bem como os dados armazenados no servidor. Custo: zero.
22	Acesso e alteração indevida de dados das provas a serem realizadas devido ao acesso não-autorizado por meio de senha de usuário.	Instituir política de senhas, definindo padrões seguros de senhas (alfanuméricos com mais de 12 caracteres) e curta periodicidade para troca de senhas. Custo: zero.
23	Acesso e alteração indevida de dados das provas a serem realizadas devido à ação de alunos mal intencionados com acesso a computadores com as menções.	Limitar o acesso físico e lógico de alunos aos computadores com as menções. Custo: 2000 reais.
24	Perda dos dados sobre projetos sociais devido à ausência de *backup* atualizado.	Instituir política de *backup* prevendo como, quem, e com que frequência será realizado o *backup*. Custo: zero.
25	Alteração/perda de dados sobre os projetos sociais devido ao acesso não-autorizado por meio de senha de usuário.	Instituir política de senhas, definindo padrões seguros de senhas (alfanuméricos com mais de 12 caracteres) e curta periodicidade para troca de senhas. Custo: zero.

Fonte: Produzido pelo autor do presente trabalho

5.4.2 Determinação dos riscos residuais

Para determinação dos riscos residuais, foi necessário reavaliar as variáveis dos riscos identificados previamente, considerando os efeitos previstos na implementação das soluções traçadas no plano de tratamento. Os riscos residuais foram recalculados e constam no Quadro 14.

Quadro 14: Riscos residuais da Educação Inovadora

Nº	Cenário de incidente	Risco	Avaliação de risco após tratamento previsto			Risco Residual
			Impacto	Probabilidade	Criticidade	
1	Comprometimento dos dados pessoais dos clientes devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Alto**	**Baixo**	**Baixo**	**Alta**	**Baixo**
2	Comprometimento dos dados pessoais dos clientes devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Alto**	**Baixo**	**Baixo**	**Alta**	**Baixo**
3	Comprometimento dos sobre desempenho pedagógico e menções de alunos devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Alto**	**Baixo**	**Baixa**	**Alta**	**Baixo**
4	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Alto**	**Baixo**	**Baixa**	**Alta**	**Baixo**

5	Comprometimento dos dados pessoais dos clientes devido à falha do sistema e ausência de *backup* atualizado.	**Médio**	**Baixo**	**Baixa**	**Alta**	**Baixo**
6	Comprometimento dos dados financeiros devido falha do sistema de pagamentos de funcionários e fornecedores e à ausência de *backup* atualizado.	**Médio**	**Baixo**	**Baixa**	**Média**	**Baixo**
7	Divulgação e/ou alteração indevida dos dados financeiros da instituição devido à invasão e captura de dados por hacker.	**Médio**	**Baixo**	**Baixa**	**Média**	**Baixo**
8	Comprometimento dos dados sobre desempenho pedagógico e menções de alunos devido a falhas técnicas e ausência de *backup* atualizado.	**Médio**	**Baixo**	**Baixa**	**Alta**	**Baixo**
9	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à ação de alunos mal intencionados com acesso a computadores com as menções.	**Médio**	**Baixo**	**Baixa**	**Alta**	**Baixo**
10	Comprometimento das provas a serem realizadas devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Médio**	**Baixo**	**Baixa**	**Média**	**Baixo**
11	Comprometimento das provas a serem realizadas devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Médio**	**Baixo**	**Baixa**	**Média**	**Baixo**

12	Comprometimento dos dados de projetos sociais devido à danificação dos equipamentos do servidor decorrente da inundação por águas pluviais das instalações.	**Médio**	**Baixo**	**Baixa**	**Baixa**	**Baixo**
13	Comprometimento dos dados de projetos sociais devido ao superaquecimento dos equipamentos do servidor decorrente da interrupção da energia dos aparelhos de ar condicionado.	**Médio**	**Baixo**	**Baixa**	**Baixa**	**Baixo**
14	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido ao acesso não-autorizado por meio de senha de usuário.	**Médio**	**Baixo**	**Baixa**	**Alta**	**Baixo**
15	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão e captura de dados por hacker.	**Médio**	**Baixo**	**Baixa**	**Alta**	**Baixo**
16	Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão pelo firewall e captura de dados por hacker.	**Médio**	**Médio**	**Baixa**	**Alta**	**Médio**
17	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixo**	**Baixa**	**Alta**	**Baixo**
18	Divulgação e/ou alteração indevida dos dados pessoais dos clientes devido à invasão e captura de dados por hacker.	**Baixo**	**Baixo**	**Baixa**	**Alta**	**Baixo**

19	Divulgação e/ou alteração indevida dos dados financeiros da instituição devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixo**	**Baixa**	**Média**	**Baixo**
20	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixo**	**Baixa**	**Alta**	**Baixo**
21	Alteração de dados/perda de dados sobre desempenho pedagógico e menções de alunos devido à invasão e captura de dados por hacker.	**Baixo**	**Baixo**	**Baixa**	**Alta**	**Baixo**
22	Acesso e alteração indevida de dados das provas a serem realizadas devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixo**	**Baixa**	**Média**	**Baixo**
23	Acesso e alteração indevida de dados das provas a serem realizadas devido à ação de alunos mal intencionados com acesso a computadores com as menções.	**Baixo**	**Baixo**	**Baixa**	**Média**	**Baixo**
24	Perda dos dados sobre projetos sociais devido à ausência de *backup* atualizado.	**Baixo**	**Baixo**	**Baixa**	**Baixa**	**Baixo**
25	Alteração/perda de dados sobre os projetos sociais devido ao acesso não-autorizado por meio de senha de usuário.	**Baixo**	**Baixo**	**Baixa**	**Baixa**	**Baixo**

Fonte – Produzido pelo autor do presente trabalho

Apenas o cenário nº 16 (Divulgação e/ou alteração indevida dos dados do sistema de pagamento de funcionários e fornecedores devido à invasão pelo firewall e captura de dados por hacker) apresenta risco residual médio mesmo após o tratamento (Contratar as funcionalidades de IPS e IDS para o firewall), isso porque a invasão pode ocorrer mesmo com essas funcionalidades (IDS e IPS) implementadas, caso a ferramenta seja mal gerenciada.

5.5 Considerações sobre a aplicação do modelo

A aplicação do modelo de gestão de riscos da segurança da informação na instituição fictícia Educação Inovadora permitiu verificar alguns benefícios que o modelo trouxe a essa escola e que pode trazer às demais organizações.

Para a Educação Inovadora, foi possível identificar cenários, antes desconhecidos, com altos riscos à segurança da informação e que podem trazer prejuízos consideráveis para a prosperidade e continuidade do negócio da instituição. A título de exemplo, verificou-se que não há sistema de escoamento de águas pluviais, de forma que no caso de chuvas torrenciais, poderá ocorrer alagamento da sala onde estão os servidores de arquivos. Caso esses servidores sejam danificados pela água, poderá resultar na perda definitiva de dados sobre clientes, funcionários, fornecedores e alunos. Com isso, a escola terá a árdua tarefa de coletar novamente os dados, o que poderá afetar negativamente a imagem da instituição.

A aplicação do modelo permitiu, portanto, conhecer os problemas relacionados à segurança da informação da Educação Inovadora e traçar ações para solucioná-los ou, ao menos, amenizá-los. Isso torna essa instituição menos vulnerável à incidência de ameaças e melhor preparada para tomar ações para minimizar os impactos resultantes de um evento adverso.

O modelo de gestão de riscos aplicado na Educação Inovadora demonstrou ser aplicável também nas demais organizações que desejam assegurar a proteção das suas informações. O modelo prevê um passo-a-passo para as atividades previstas em cada etapa da gestão de riscos. Ademais, os critérios de referência pré-definidos para atividades que envolvem análises qualitativas facilitam sua execução e reduzem a subjetividade inerente ao processo.

A implementação de um modelo de gestão de riscos pelas organizações, como o proposto no presente trabalho, demonstra um empenho da alta gestão com relação à segurança das informações e envolve um grande número de setores e colaboradores, o que acaba por desenvolver a cultura de proteção. Quanto maior a percepção dos colaboradores sobre a necessidade de proteger as informações, menos vulnerável a instituição estará com relação as ameaças à integridade, confidencialidade e disponibilidade de suas informações.

CONCLUSÃO

A proteção das informações de valor para as organizações contra as ameaças à sua integridade, disponibilidade e confidencialidade tornou-se atividade fundamental para assegurar a continuidade e prosperidade do negócio. A gestão de riscos de segurança da informação mostra-se uma alternativa eficaz para proteger essas informações.

A ISO publicou, em 2011, a norma 27005, que traz recomendações para gestão de riscos de segurança da informação. Contudo, a norma trata genericamente da gestão de riscos e delega às organizações a escolha da metodologia para algumas atividades tais como avaliação das consequências, avaliação da probabilidade e determinação do nível de risco. Para as organizações que ainda não implementaram a gestão de riscos ou que não possuem experiência na área de segurança da informação, as recomendações da ISO podem não ser suficientes para que tenham êxito na utilização dessa ferramenta.

Esta pesquisa buscou elucidar e simplificar as recomendações da ISO, de forma a propor um modelo simples, prático e que possa ser facilmente integrado à rotina da organização. Para tanto, foi necessário ajustar atividades recomendadas pela ISO e definir parâmetros qualitativos de análise dos riscos e de seus componentes. A aplicabilidade do modelo mostrou ser viável, tomando como base o estudo de caso de uma organização fictícia (Educação Inovadora), por meio do qual foi possível conhecer os riscos à segurança da informação e propor soluções para reduzi-los ao menor nível possível. O estudo de caso permitiu, além de validar o modelo proposto, facilitar o entendimento das atividades previstas no processo de gestão de riscos de segurança da informação.

Com base na demonstração do modelo proposto, verificou-se ser possível aplicá-lo também a outras organizações, sobretudo àquelas que não possuem um modelo de gestão de riscos implementado ou que não possuem experiência na área de Segurança da Informação. A proposta do modelo é constituir-se um primeiro passo para as organizações implementarem a gestão de riscos de segurança da informação e aprimorá-lo à medida que adquirirem experiência nessa área.

Assim, alcançou-se o objetivo proposto nesta pesquisa qual seja o de formular um modelo prático de gestão de riscos de segurança da informação para as organizações.

Não houve a intenção de se esgotar a temática da gestão de riscos de segurança da informação, restando alguns aspectos que podem ser estudados e melhorados em pesquisas acadêmicas futuras:

- Análises quantitativas de riscos e de seus fatores ou outras análises que permitam reduzir a subjetividade das medições qualitativas utilizadas na pesquisa.
- Elaboração de listas de controles de segurança, a ser utilizada tanto para identificar e avaliar os controles existentes como para propor controles para mitigar riscos. Essas listas podem auxiliar também na identificação de vulnerabilidades.
- Desenvolvimento de softwares capazes de automatizar e gerenciar as atividades previstas no modelo proposto de gestão de riscos.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas. **NBR ISO GUIA 73 Gestão de riscos – Vocabulário.** Rio de Janeiro, 2009.

_____. **NBR ISO/IEC 27001:2013 Sistema de gestão de segurança da informação – requisitos**. Rio de Janeiro, 2013.

_____. **NBR ISO/IEC 27005:2011 Gestão de risco de segurança da informação**. Rio de Janeiro, 2011.

BEAL, A. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. **Metodologia Científica**. São Paulo: Person Prentice Hall, 2002.

COSTA, Eliezer Arantes da**; Gestão estratégica**. São Paulo: Saraiva, 2002.

International Organization for Standardization. **ISO/IEC 27000:**2014 *Information security management systems — Overview and vocabulary.* Genebra, 2014.

National Institute of Standards and Technology. **Guide for Conducting Risk Assessments**. Gaithersburg, 2012.

_____. ***Managing Information Security Risk:*** *Organization, Mission, and Information System View*. Gaithersburg, 2011.

SÊMOLA, M. **Gestão da Segurança da Informação:** uma visão executiva. Rio de Janeiro: Elsevier, 2003.

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores:** princípios e práticas. Edição Campus. 2. ed. Rio de Janeiro: Elsevier, 2014.