GESTÃO DE RISCO DA INFORMAÇÃO BASEADO NA ISO/IEC 27005/2008

INFORMATION RISK MANAGEMENT BASED ON ISO / IEC 27005/2008

FERNANDO MACEDO TRONCHA
Especialista em Gestão e Segurança em Redes de Computadores pela Universidade Estadual de Goiás (UEG), Campus de Trindade
fernandomt1982@gmail.com

FÁBIO BARBOSA RODRIGUES
Mestre e doutorando em Engenharia Elétrica e de Computação pela UFG - Universidade Federal de Goiás (Goiânia / GO) e docente da UEG - Universidade Estadual de Goiás (UEG), Campus de Trindade
prof.fabiobrodrigues@gmail.com

Resumo: Este artigo trata de um modelo preliminar de análise/avaliação de risco de segurança da informação capaz de identificar os riscos de uma instituição de ensino, tais como: falha no ingresso de alunos na escola, falha no acesso ao sistema por falta de cadastro de perfil de usuário de acordo com suas funções, falha de software, falta de conhecimento do sistema. A análise/avaliação de risco é uma atividade do processo de gestão de risco em que são identificados os riscos e seus componentes - ativos, ameaças, vulnerabilidade e consequências. O trabalho apresenta um caso prático de gestão de risco com base na norma ABNT ISO/IEC 27005/2008.
Palavras-chave: Gestão de Risco. Segurança da informação. ABNT ISO/IEC 27005/2008.

Abstract: This article deals with a preliminary model of information security risk analysis / evaluation capable of identifying the risks of an educational institution, such as: failure to enroll students in school, access to the system due to lack of profile profile User according to the functions, software, system knowledge. Risk analysis / assessment is an activity of the risk management process in which risks and their components - assets, threats, vulnerability and consequences are identified. The work presents a risk management model based on ISO / IEC 27005/2008.
Keywords: Risk Management. Information Security.Standard ABNT ISO / IEC 27005/2008.

INTRODUÇÃO

A informação possui um valor altamente expressivo e representa poder para quem a possui, assim, a proteção da informação e do conhecimento é de vital importância para a sobrevivência das organizações.

> Neste cenário onde a informação se tornou um dos principais ativos de uma organização, o controle e proteção desta informação tornaram-se objeto de estudo e investimento tecnológico, objetivando a criação de novos métodos e ferramentas de sua gestão(SAMPAIO, 2014, p.9)

O acesso aos dados corporativos através dos sistemas de informação atrai os invasores e espiões, por isto, as organizações dependem cada vez mais dos seus sistemas para sua proteção.

A preocupação com a proteção da informação como ativo no âmbito das organizações criou a necessidade de sistematização e padronização dos conceitos de segurança da informação, de forma a consolidar as bases para o desenvolvimento seguro e uniforme de soluções para os problemas emergentes dessa questão, assim criou-se diversas normas nas séries da ISO 27000.

Para gerir a segurança da informação, segundo estas normas, inicialmente deve-se realizar o estudo de gestão de risco. Trata-se de uma metodologia que procura evitar que riscos e ameaças se concretizem e gere prejuízos a organização. Uma gestão eficaz de riscos reduz as chances e a gravidade de incidentes de segurança, ou seja, uma forma de proteção para que se evitem riscos e vulnerabilidades da informação.

O objetivo deste trabalho é apresentar o processo de gestão de risco com uma análise/avaliação da instituição de ensino visando observar os principais riscos que envolvem uma instituição de ensino, e a partir dos resultados definir as prioridades em relação às providências a serem tomadas para afastar/erradicar os riscos do estabelecimento.

GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

A norma da Associação Brasileira de Normas Técnicas (ABNT) ISO/IEC 27005/2008 fornece diretrizes e descreve um processo genérico para a Gestão de Risco de Segurança da Informação de uma organização. Esta Norma cobre a Gestão de Riscos de Segurança da Informação e foi criada em 2008, mas foi tecnicamente revisada em 2011, onde o texto editado nesta data passou a prevalecer sobre o outro. O processo de Gestão de Risco de Segurança da Informação (GRSI) é um processo contínuo, ou seja, trata-se de um ciclo de melhoria ininterrupta. Este processo, definido por esta norma, pode ser aplicado tanto a uma organização como a um projeto isolado, com isto é possível a utilização do processo de GRSI em várias circunstâncias.

Alguns conceitos orientam o entendimento da estrutura da ISO/IEC 27005 servindo de parâmetros para todos os tipos de organizações que pretendam gerir os riscos que afetariam a segurança da informação da organização. É importante destacar algumas definições elencadas pela ISO/IEC 27005:

Risco de segurança da informação é:

> O risco de segurança da informação que está associado com o potencial de que ameaças possam explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e,consequentemente, causar dano a uma organização (NBR ISO/IEC 27005, 2011).

Deste conceito percebemos que alguns termos merecem destaque, tais como:ameaça,vulnerabilidade, ativo e danos. Também devem ser enfatizados outros conceitos pertinentes à gestão de risco de segurança da informação, quais sejam:

Ameaça “é a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização” (ABNT ISO/IEC 27005, 2011).

Vulnerabilidade “é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (ABNT ISO/IEC 27005, 2011).

Ativo “é algo que tem valor para a organização” (ABNT ISO/IEC 27005, 2011).

Dano ou impacto “é a mudança adversa no nível obtido dos objetivos de negócios” (ABNT ISO/IEC 27005, 2011).

A norma utiliza o termo "consequência" para fazer referência às perdas operacionais relativas à proteção de ativos. As palavras "impacto e consequência são empregadas na norma para se referirem aos danos causados a organização devido à perda ou comportamento de ativos" (ABNT ISO/IEC 27005, 2011).

Por outro lado, há alguns termos que são aplicados pela legislação que tem significado específicos, como: "comunicação do risco" que é a troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas; "avaliação de risco” que é o processo de comparar os resultados da análise de risco com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

Podemos mencionar os termos "identificação de riscos" como sendo o processo para localizar, listar e caracterizar elementos do risco; "tratamento de risco" como sendo o processo de seleção e implementação de medidas para modificar um risco e por fim, "gestão de risco" que é a atividade coordenada para dirigir e controlar uma organização no que se refere a riscos.Há ainda outros termos definidos pelas normas, mas estes são os principais que irão subsidiar este estudo.

PROCESSO DE GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

Nos dizeres de Sampaio (2014, p. 25) “o risco é entendido como alguma coisa que cria possibilidades ou produz danos, ou seja, são circunstâncias que geram ou agregam potencialidade de perdas e danos”. Este risco é quantificável por meio da possibilidade de um evento acontecer e causar perdas.

Gerenciar os riscos é um dos principais processos da gestão de segurança da informação, pois objetivaa identificação, avaliação e priorização de riscos, com objetivo de minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, reduzindo o risco a um nível aceitável.

O processo de gestão de risco é definido por algumas atividades, quais sejam: definição do contexto; análise/avaliação de riscos de segurança da informação; tratamento do risco de segurança da informação; aceitação do risco de segurança da informação; comunicação do risco de segurança da informação; monitoramento e análise crítica de riscos de segurança da informação (figura 1).

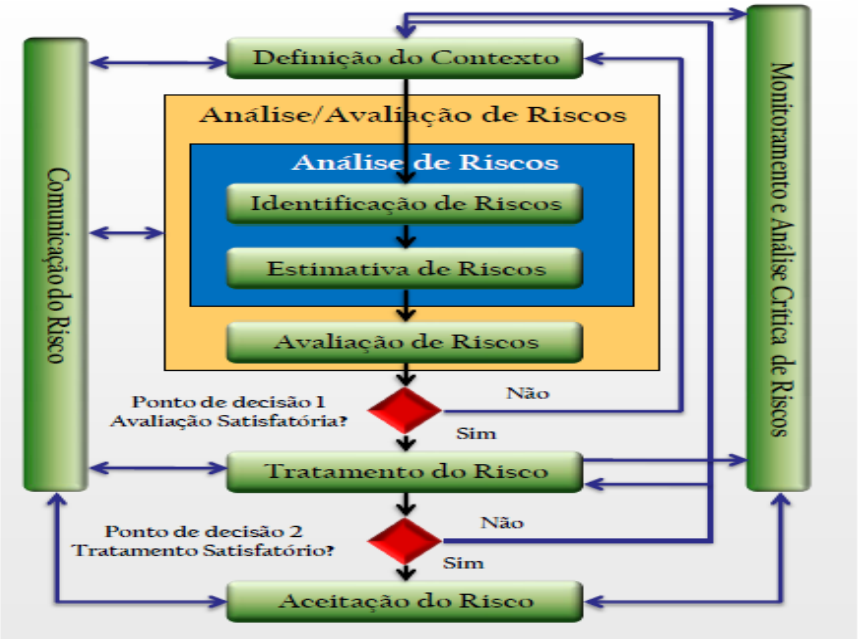

Figura 1: Apresenta a ligação entre as atividades do processo de GRSI
Fonte: NBR ISO/IEC 27005, 2011.

No processo de gestão de riscos de segurança da informação primeiramente define-se o contexto, onde se indica o alvo cuja gestão de risco vai proceder. Para a definição do contexto é importante ter todas as informações da organização, identificando os objetivos e limites do GRSI e quem irá executar o processo de GSRI.

Posteriormente, executa-se um processo de análise/avaliação de riscos. Para Sampaio (2014, p.22) a análise/avaliação de riscos tem o papel de identificar, quantificar ou descrever qualitativamente os riscos, priorizados de acordo com os objetivos relevantes da organização.

> Esta atividade recebe como entrada os critérios básicos, o escopo e os limites, e a organização do processo de GRSI que se está definindo. Como saída é gerada uma lista de riscos avaliados, ordenados por prioridade de acordo com os critérios de avaliação de riscos (SAMPAIO, 2014, p. 22).

Após a organização conhecer o nível de risco ela poderá decidir o que fazer em relação ao risco: modificar, reter, evitar e compartilhar, até que se chegue à decisão aceita pela organização para se traçar um plano de tratamento do risco. No tratamento do risco faz-se uma lista de risco ordenada por prioridade de acordo com os critérios de avaliação de riscos associada aos cenários de incidentes que os provocam; e como resultado é confeccionado um plano de tratamento do risco e de riscos residuais, suscetível ao aceite dos gestores da organização.

A aceitação do risco é:

> [...] a formalização pela autoridade competente da decisão de aceitar o risco. Os gestores da organização devem analisar o plano de tratamento do risco e os riscos residuais e, no caso de aprovação dos mesmos, as condições associadas à aprovação devem ser registradas (SILVA, 2009, p.27).

É importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados. Informações sobre os riscos identificados podem ser muito úteis para o gerenciamento de incidentes e pode ajudar a reduzir possíveis prejuízos.

Os resultados detalhados de cada atividade do processo de gestão de risco de segurança da informação, assim como o processo de avaliação de risco e sobre o tratamento do risco devem ser documentados. (ABNT ISO/IEC 27005, 2011).

“A comunicação do risco são trocas compartilhadas entre o tomador de decisões e/ou as outras partes interessadas” (ABNT ISO/IEC 27005, 2011), ou seja, a comunicação é bidirecional.

A última atividade do processo de GRSI, é o monitoramento e análise crítica de riscos da segurança da informação, prevê que os riscos sejam monitorados e analisados criticamente a fim de identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de manter uma visão geral sobre os riscosABNT ISO/IEC 27005 (2011).

ESTUDO DE CASO

Este trabalho apresenta a aplicação da norma ISO/IEC 27005/2008 em um ambiente real. Foi realizado um estudo de caso em uma instituição de ensino. Esta instituição de ensino possui cinco unidades, onde todas foram analisadas. Em cada unidade possui cerca de 30 professores e 20 servidores da área administrativa e correlata, e aproximadamente 450 alunos que estão matriculados entre o pré-escolar e o 9º ano, além da constante presença dos pais nas atividades educacionais.

A estrutura física de cada unidade é bastante similar, conforme figura abaixo, onde ilustramos com a Maquete da Escola Aprendizes.

São dois blocos de prédio divididos por um gramado. No bloco A ficam os alunos do pré-escolar até o 5º ano e no bloco B ficam os alunos do 6º ano ao 9º ano. O setor administrativo fica em um terceiro prédio da entrada na instituição onde está a coordenação, direção, secretaria, biblioteca, sala de professores, entre outras salas administrativas e ao fundo uma quadra esportiva e um refeitório (figura 2).

Figura 2: Maquete da Escola Aprendizes
Fonte: Autores (2016).

DEFINIÇÃO DO CONTEXTO

- Identificação da Organização: Escola Aprendizes, localizada na Rua das Pedras n. 100, Centro, Goiânia, Goiás. (Os dados são de uma escola real, mas por questões jurídicas não foi autorizado a sua publicação.)

- Limite do escopo: A gestão de risco será limitada aos ativos de tecnologia da informação (TI) específicos de acesso dos alunos, professores, gestores e pais no ambiente físico e virtual da instituição de ensino.

- Ativos de Informação: A escola possui um gerenciamento de presença e plano de aula, gerenciamento das atividades complementares, controle de perfil de usuários,

controle de acesso de alunos na instituição. Os ativos citados a seguir dão suporte a estas atividades:

* Sistema Integrado de Gestão de Atividades Acadêmicas (SIGAA): sistema completo com diversas funcionalidades, responsável por matrículas e contratos, gerenciamento de notas, relatórios, recibos.

* Sistema de Acesso de Alunos (SAA): é um sistema responsável pela entrada e saída de alunos na instituição, onde os pais e professores identificam se os alunos estão na escola através de um sistema Web, além de gerar automaticamente a presença dos alunos no plano de aula.

* Acesso de Controle de Usuário (ACU): é uma funcionalidade do sistema informatizado onde o usuário tem acesso apenas ao perfil de sua função.

CRITÉRIOS BÁSICOS

Critérios para avaliação de risco:

A tabela abaixo será utilizada como referencial para ordenar as prioridades dos riscos da instituição de ensino no que tanque a tecnologia da informação. Os cenários de incidentes que tenham o nível de risco (NR) mais elevado devem ser considerados primeiro.

Os riscos graves (tabela 1) são aqueles que envolvem perda de autenticidade, confidencialidade, integridade e disponibilidade das informações, e todos aqueles que causem dano à imagem da instituição de ensino.

- **Critério para aceitação de risco**

Tabela 1: - Nível de Risco

Nível de Risco	Descrição Aceitabilidade	Aceitabilidade
Alto(16-25)	Paralisação do serviço da escola por completo.	Inaceitável, requer ação imediata para correção do risco
Médio(5-15)	Alguns processos afetados	Não pode ser aceito, requer correção para resolver o risco
Baixo(1-4)	Efeitos menores	Risco aceitável

Fonte: Autores (2016)

(As medidas são empíricas com medições subjetivas. É importante que a organização utilize um método com o qual ela se sinta confortável, com resultados reproduzíveis)

- **Análise de Risco**

O nível de risco (NR) é calculado com a multiplicação do nível de impacto (NI) pelo nível de probabilidade (NP) (tabelas 2 e 3).

Tabela 2: Análise de Risco

ANÁLISE DE RISCOS								
N	Sistema	Identificação De Riscos			Estimativa de riscos			Tratamento do Risco
		Ameaça	Vulnerabilidade	Impacto	NP	NI	NR	TR
1	SIGAA	Comprometimento da disponibilidade	Falha nos servidores	Perda da disponibilidade dos dados	2	3	6	Espelhamento e Backup do banco de dados em outro servidor
2	SIGAA	Falha de software	Não confecção automática de arquivos	Perda de disponibilidade e autenticidade	4	4	16	Geração automática de arquivos através de dados do sistema.
3	ACU	Sistema permite usuários logar em todos os perfis	Alunos e professores podem logar em perfis diversos	Perda de confidencialidade	5	4	20	Controle de perfis de usuários
4	SIGAA	Erro durante o uso	Interface de usuário complicada	Perda de eficiência	3	3	9	Treinamento periódico
5	SAA	Comprometimento no acesso	Pessoas podem entrar e sair da escola sem identificação	Perda integridade e confidencialidade	5	5	25	Confecção de carteiras com a tecnologia RFid
6	ACU	Abuso de direito	Não execução de Logout ao se deixar uma estação de trabalho desassistida	Perda de confidencialidade	5	3	15	Implementação no sistema de logout automática após 2 minutos desassistida
7	ACU	Forjamento de direito	Gerenciamento de senhas mal feitas	Perda de confidencialidade, integridade e disponibilidade de dados	2	5	10	Criação de senhas com caracteres especiais, letras e números conjuntamente
8	SIGAA	Software novo ou imaturo	Defeito de software	Perda de confidencialidade, integridade e disponibilidade de dados	2	4	8	Realização de testes para implementação da fase final
9	Recursos humanos	Treinamento insuficiente	Erro durante o uso de software	Perda de confidencialidade, integridade de dados	3	4	12	Treinamento periódico equipe

Fonte: Autores (2016).

Tabela 3: Lista de riscos ordenados por prioridades

CENÁRIO DE RISCO	NR
Acesso irregular de alunos devido à falta de gerenciamento dos acessos	25
Comprometimento do ACU nos perfis dos usuários tendo acesso a várias funcionalidades não restritas a sua função.	20
Comprometimento no SIGAA por falha de software, onde não gerava automaticamente arquivos como: contratos, recibos.	16
Comprometimento no ACU, quando não há o logout do usuário ao deixar uma estação de trabalho desassistida	15
Erro durante o uso de software por treinamento insuficiente	12
Gerenciamento de senha mal definida	10
Má utilização do sistema por desconhecimento e alegação de interface complicada	9
Defeito no software por ser um software novo em fase de alguns testes	8
Comprometimento na disponibilização do SIGAA devido à falha nos servidores	6

Fonte: Autores (2016)

Após a identificação dos elementos constitutivos do risco chega-se por meio de uma análise/avaliação de risco a uma lista ordenada por prioridade de riscos para o tratamento.

TRATAMENTOS DOS RISCOS

Depois de identificados os riscos far-se-ão o tratamento dos três principais riscos para verificar se serão aceitáveis ou não.

As opções de tratamento que melhor se enquadra para os três maiores riscos são: para o caso de acesso irregular de alunos na instituição de ensino é a confecção de carteiras com a tecnologia RFid ("Radio-*FrequencyIDentification*" ou identificação por radiofrequência) com controle de entrada e saída de alunos e funcionários na escola (figura 3).

Para o segundo risco apurado na lista de prioridades verifica-se a necessidade de cada usuário ter acesso apenas ao perfil da sua função, bloqueando as demais funcionalidades. Assim, foi implementado ao sistema o controle de perfis para os usuários, onde cada pessoa tem acesso restrito à sua área de atuação (figura 4).

Figura 3:Exemplo de Carteira Estudantil com Tecnologia RFID
Fonte: Autores (2016)

Figura 4: Print da Tela do Computador com imagem dos controles de perfis da EscolaAprendizes
Fonte: Autores (2016)

Por fim, para resolver a falha de software a fim de aperfeiçoar o tempo dos servidores da instituição de ensino, foi implementado a geração automática de contratos, boletos, recibos, relatórios e outros documentos administrativos, através dos dados cadastrais realizados quando da matrícula do aluno na instituição de ensino (figura 5).

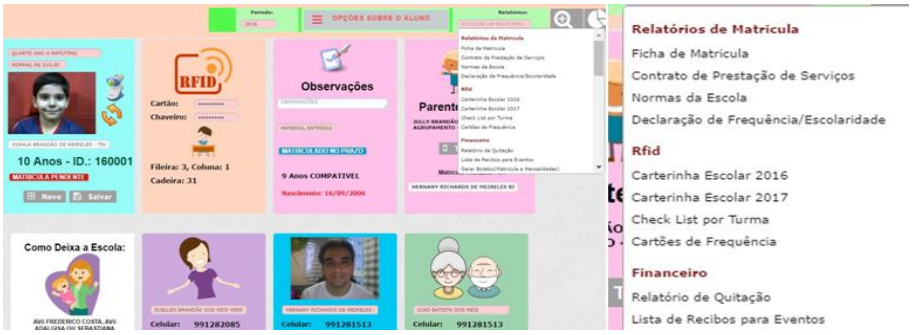

Figura 5: Print da Tela do Computador com imagem dos relatórios da Escola Aprendizes
Fonte: Autoria própria (2016)

A instituição de ensino implementando estes novos tratamentos: - conseguiu estar com o seu sistema de gestão sempre em funcionalidade e otimizado, - erradicar o acesso de usuários a perfis não autorizados, - extinguir a insegurança da presença/ausência do aluno no estabelecimento educacional. Após estes ajustes o risco foi considerado aceitável.

Como exposto acima, estes riscos são estáveis, mas estão constantemente mudando, com isto os gestores do sistema de gestão das intuições de ensino adotaram a prática de análise/avaliação de riscos periodicamente para afastar riscos que podem prejudicar o negócio.

CONCLUSÃO

A Escola Aprendizes serviu para que aplicássemos as etapas do processo de GRSI segundo a norma ISO/IEC 27005/2008.

Os resultados obtidos indicaram a possibilidade de um método de análise-avaliação dos riscos capaz de atender toda a instituição afastando os riscos mais recorrentesreferente aos Sistemas Integrados de Gestão de Atividades Acadêmicas, Sistema de Acesso de Alunos, Acesso de Controle de Usuário, quais sejam: acesso irregular de alunos na instituição de ensino, perfis dos usuários não restritos à sua área de atuação e falha de software.

A facilidade de compreensão do processo e de seus resultados, a velocidade e o baixo custo em relação a uma análise de riscos são as vantagens desta avaliação. Sabe-se que para tal processo se precisa de uma disponibilidade orçamentária da instituição, um planejamento antecipado dos gastos, e isto reforça a necessidade de um método simples e eficaz que aponte os principais riscos de segurança da informação.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001**: Sistema de gestão da segurança da informação. Rio de Janeiro, 2013.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002**: Código de Prática para a gestão da segurança da informação. Rio de Janeiro, 2014.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27003**: Implementação do sistema de gestão de segurança da informação. Rio de Janeiro, 2011.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27004**: Implementação do sistema de gestão de segurança da informação. Rio de Janeiro, 2010.

Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27005**: Técnicas de segurança do sistema de gestão da informação. Rio de Janeiro, 2011.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2007.

MENEZES, Josué das Chagas. **Gestão da Segurança da Informação**. Leme, SP: Mizuno, 2006.

SAMPAIO, DhiegoRhubens Lima. **Um estudo sobre Riscos de Segurança da informação no Campus da UFC em Quixadá com base na norma ISO/IEC 27005**. 2014.

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

SILVA, Pedro Jorge Sucena. **Análise/Avaliação de Riscos de Segurança da Informação para a Administração Pública Federal: um enfoque de alto nível baseado na ISO/IEC 27005**.2009.