*Journal of Internet Services and Applications, 2023, 24:6,* doi: 10.5753/jisa.2023.xxxxx

Cc.logo.circle.svg This work is licensed under a Creative Commons Attribution 4.0 International License.

# Gestão de riscos em TI: os impactos organizacionais de relativos à má gestão.

Marcos Gabriel Koslovski Santos [iD icon](https://orcid.org/0000-0002-0339-6624) 🖂 [ Faculdade Dom Bosco de Porto Alegre |

marcosgabriel62@gmail.com]

🖂 Curso de Sistemas de informação*, Faculdade Dom Bosco de Porto Alegre, R. Mal. José Inácio da Silva, 355, Passo d'Areia, Porto Alegre, RS, 90520-280, Brazil.*

Received: DD Month YYYY • Accepted: DD Month YYYY • Published: DD Month YYYY

Abstract. Diante das constantes evoluções e de um mundo cada vez mais informatizado criam se gigantescas oportunidades de crescimento organizacional e incremento de receitas, advindos da tecnologia cada vez mais avançada. A TI das organizações tem papel intimo neste cenário e se faz necessária para alinhar essas novas tecnologias e possibilidades as expectativas de negocios das organizações. No entanto, ela deve estar sempre alinhada também a uma gestão de riscos em TI concisa e de acordo com o apetite de riscos da organização como um todo. Ao longo deste artigo vamos abordar os impactos negativos possíveis a uma organização relacionados a má gestão de riscos em TI.

Palavras chave: Gestão de riscos, TI, Tecnologia da Informação, Evolução constante, Melhoria continua.

## Introdução

Por muito tempo a TI das empresas não era vista como parte estratégica e importante ao negocio e ao produto, porém nos tempos atuais as coisas mudaram. Hoje, se a empresa não investe e aplica em recursos de TI a mesma torna-se obsoleta, e isso pode causar diversas consequências em suas atividades de negócio, inclusive levando a empresa a declarar falência devido a falta de competitividade frente a suas concorrentes.

Com o crescente uso de tecnologia nas organizações, por consequência cresce também os riscos envolvidos em suas operações. Sabendo disso, juntamente com essa evolução dos recursos e tecnologias outra área cresceu e se desenvolveu esta chamada de gestão de riscos em TI.

A gestão de riscos em TI vem então para alinhar estes riscos ao apetite a riscos da organização, avaliando-os, priorizando-os, considerando seus impactos nas atividades da empresa, aplicando controles a fim de mitigar as suas potenciais consequências e conferindo qualidade aos serviços ou produtos entregues pela organização.

No entanto, por mais disponível que as ferramentas estejam ainda existem empresas que não as utilizam e (ou) as utilizam incorretamente, o que traz sérios riscos ao pleno funcionamento da organização.

Mas, sabendo em linhas gerais o que a gestão de riscos em TI faz, quais são as consequências de uma possível má gestão de recursos em ti? Ao longo desse artigo estaremos discutindo sobre algumas das possíveis consequências em uma organização com a gestão de riscos em mau funcionamento.

## Alinhamento e padronização

Quando falamos da gestão de riscos em TI, falamos de uma grande área munida de diversas ferramentas e frameworks que trata dos riscos envolvidos e ligados a TI na operação de uma organização.

Regidos pela NBR27001 e NBR27005 os responsáveis pela área de gestão de riscos de TI de uma organização devem de forma sistemática e continua identificar, analisar, avaliar e mitigar os riscos a fim de não expor a organização mais do que o apetite a riscos que ela está disposta a se submeter para conquistar seus objetivos.

Estes conjuntos de normas aliados a um framework de gestão e governança em TI como o COBIT, por exemplo, permitem a uma completa gestão de riscos em TI.

Mas, existem casos e casos. Nem todas as empresas que se utilizam de TI para apoio a seus negócios possuem toda a estrutura de governança de TI formada.

Às vezes a estrutura formada comete erros catastróficos também, expondo de forma acidental ou proposital a organização inteira a riscos maiores do que ela estava disposta a se submeter.

Um risco mal calculado ou mitigado a depender de sua criticidade representa uma grande ameaça a uma organização, sendo que muitas empresas já vieram a encerrar suas operações por conta de erros em relação à gestão de riscos. Dessa forma, reforça-se a necessidade e a importância da regulação, da normatização e do consumo das tantas ferramentas disponíveis para a gestão de riscos em TI. A seguir falaremos dos impactos que uma organização está sujeita no caso de uma má gestão de riscos de TI.

## Os impactos

### 3.1 O fim das operações

Dentre os impactos da má gestão de riscos citamos em primeiro lugar o julgado pela maioria como o pior deles que é o termino das operações. Usamos como exemplo a Knight Capital Group, que conforme matéria na revista exame (“Knight Capital perde US$440 milhões por falha em robô”, 2012) a empresa americana que operava na bolsa de valores sofreu perdas milionárias em 2012 devido a um erro de sistema, desenvolvido e colocado em produção sem os testes apropriados.

Sabendo que um erro como o que ocorreu poderia causar a ruina da empresa, entende-se que qualquer desenvolvimento que pudesse causar danos catastróficos deveria ser testado exaustivamente antes de ser colocado em produção, correto? É o correto, mas não foi o que ocorreu. Em algum momento a gestão de riscos de TI falhou ao permitir que o erro fosse colocado em produção.

Tal erro levou ao fim das operações da empresa como ela era e a sua venda a outra companhia apenas um ano após o ocorrido. Seria esta a maior perda financeira por conta da má gestão de riscos em TI? Não, e está longe de ser.

### 3.2 Prejuízos financeiros

Os possíveis prejuízos financeiros ligados à má gestão de riscos em TI parecem se confundir com o fim das operações, mas sim se confundem mesmo.

O extremo dos prejuízos financeiros é de fato o término das operações. Mas, nem sempre a empresa chega a “quebrar” devido a esses prejuízos. Às vezes ela só amarga anos de balanços no vermelho por conta de algum erro causado por essa má gestão.

Desta vez usamos como exemplo a Sony Pictures, que em 2014 sofreu um ataque cibernético em grande escala onde milhares de terabytes de dados foram vazados na internet, causando milhões de dólares em prejuízos com custos de recuperação dos dados, vazamento de filmes inéditos, dados de funcionários, e-mails e outras informações sensíveis. Em época, especialistas falavam em prejuízos entre cem e duzentos milhões de dólares, valores estes que poderiam ter sido muito menores ou até mesmo inexistentes se a gestão de riscos em TI tivesse identificado corretamente a ameaça e o potêncial da mesma e a mitigado.

### 3.3 Prejuízos à imagem

O prejuízo financeiro não foi o único impacto sentido pela Sony após o vazamento. A mesma também sofreu uma grande crise devido a falta de confiança do mercado, interrupção momentânea em suas operações devido a falta de um plano de contingência e dificuldades comerciais causadas pela exposição de e-mails trocados entre funcionários e executivos da companhia, que por muitas vezes citavam empresas, figuras públicas e astros de hollywood de forma vexatória e desrespeitosa.

Algumas empresas expostas a condições semelhantes de vazamentos de dados acabam por nunca se recuperarem plenamente, podendo até não “quebrar”, mas tendo seus resultados e rendimentos impactados para sempre.

### 3.4 A perda de dados

Os atentados de 11 de setembro de 2001 mudaram a vida de praticamente todos nós e também a gestão de riscos em TI para sempre. A proteção de dados, que é parte vital das empresas e é englobada pela gestão de riscos jamais iria prever que por conta dos atentados tanto o dado original quanto o backup, que em muitas empresas estava sendo realizado em servidores na torre vizinha, seriam destruídos juntos.

Muitas empresas deixaram de existir trazendo prejuízos incalculáveis a seus donos e clientes que viram documentos e dados únicos serem extintos.

Desta forma, a partir do 11 de setembro diversas medidas foram tomadas a fim de que problemas semelhantes não acontecessem novamente, como a descentralização do site de backup, levando os servidores de backup para outra região ou zona diferente dos servidores principais.

Usamos como exemplo um dos casos mais extremos que conhecemos, mas temos exemplos nos dias de hoje que a perda de dados relativa a algum ataque ou até mesmo falha em algum servidor foi tão catastrófica quanto.

### 3.5 Judicialização por terceiros

Em 2022 foi noticiado um vazamento de dados no Banco Pan onde em torno de 17 milhões de clientes tiveram seus dados vazados, devido segundo a empresa uma fragilidade em um de seus fornecedores.

Dados de cartão de crédito, nome e endereço de clientes foram expostos na internet, abrindo a possibilidade de golpes e compras não autorizadas feitas por terceiros.

O vazamento de dados sensíveis aos clientes pode levar o banco a ser acionado tanto por clientes que por um acaso vierem a sofrer golpes quanto pelo poder público, que irá investigar e cobrar se os marcos regulatórios estavam sendo cumpridos quando o vazamento aconteceu.

### 3.6 Não conformidades com marcos e leis regulatórias

Como citado anteriormente, a má gestão de riscos na área de TI pode fazer com que a empresa não satisfaça os requisitos mínimos em relação a leis e marcos regulatórios instituídos pelos governos dos países onde as organizações operam.

A não conformidade pode levar a multas altíssimas, aplicadas pelos órgãos reguladores e governos locais que em casos mais extremos podem até mesmo obrigar a organização a encerrar as operações de forma parcial ou total.

### 3.7 Queda na produtividade e não atingimento dos objetivos instituídos pela organização

É nítido que a produtividade e os objetivos da organização podem vir a não ser atingidos devido aos impactos citados anteriormente. Fica difícil satisfazer e atingir os objetivos da organização quando ela tem o desempenho afetado por prejuízos financeiros, prejuízos causados a sua imagem, vazamento de dados, perda de dados e não conformidade com marcos legais. Tudo isso cria um ambiente de baixas possibilidades de atingimento de qualquer tipo de meta ou expectativa.

## Conclusão

Este artigo descreveu e explicou de forma breve os diferentes impactos e consequências de uma má gestão de riscos em TI.

Ficou ainda mais evidente a necessidade de uma política sólida de gestão de riscos, clara e alinhada com os negócios da organização, a fim de mitigar e minimizar os riscos e garantir a continuidade dos negócios da empresa.

A aplicação de uma política funcional de gestão de riscos em TI envolve uma série de fatores e processos, mudanças físicas e psicológicas que devem ser implementadas, continuamente melhoradas e monitoradas de forma que os impactos referentes a uma má gestão nunca venham a serem riscos reais para a organização.

Infelizmente não há garantias de que uma empresa possa sobreviver as consequencias citadas, considerando a história e os casos conhecidos de falhas na gestão de riscos de TI. Os eventos catastróficos mudaram a realidade de muitas das empresas que conhecemos, ou costumávamos conhecer, para sempre. Portanto, é fundamental que as organizações aprendam com esses exemplos e estejam preparadas para lidar com os desafios e ameaças no ambiente digital.

Uma empresa que aplica a gestão de riscos em TI de forma correta pode vir a terminar com suas operações devido a outros fatores, mas com pouquíssimas chances de ser em decorrência de falhas relativas a algum processo ou fornecimento de TI.

# **Bibliografia**

**Banco Pan confirma vazamento de dados de clientes na área de cartões**. Disponível em: <https://tecnoblog.net/noticias/2022/04/15/banco-pan-confirma-vazamento-de-dados-de-clientes-na-area-de-cartoes>. Acesso em: 25 jun. 2023.‌

NETO, P.; ARAÚJO, W. **SEGURANÇA DA INFORMAÇÃO**. 1. ed. [s.l: s.n.]. v. 1p. 160

LENTO, L. O. **Gestão de Risco em Tecnologia da Informação**. 1. ed. Palhoça: UnisulVirtual, 2012. v. 1p. 136

‌

MIOZZO, J. **WikiLeaks reúne os melhores e-mails vazados da Sony Pictures; confira**. Disponível em: <https://www.infomoney.com.br/consumo/wikileaks-reune-os-melhores-e-mails-vazados-da-sony-pictures-confira/>. Acesso em: 25 jun. 2023.

REUTERS, D. **Ataque contra a Sony Pictures deve custar US$ 100 mi, diz especialista**. Disponível em: <https://g1.globo.com/tecnologia/noticia/2014/12/ataque-contra-sony-pictures-deve-custar-us100-mi-diz-especialista.html>. Acesso em: 25 jun. 2023.

‌

FOLHAPRESS. **Ataque hacker à Sony expôs dados pessoais de estrelas de Hollywood**. Disponível em: <https://www.gazetadopovo.com.br/economia/ataque-hacker-a-sony-expos-dados-pessoais-de-estrelas-de-hollywood-eh1jf9sbtaj6yn6flssm6ljda/>. Acesso em: 23 jun. 2023.

‌

**Knight Capital perde US$440 milhões por falha em robô**. Disponível em: <https://exame.com/invest/mercados/knight-capital-perde-us-440-milhoes-por-falha-em-robo/>. Acesso em: 23 jun. 2023.

**Como o 11/9 mudou a trajetória da proteção de dados - Aliança TI**. Disponível em: <https://www.aliancatecnologia.com/conteudo/2015/09/como-o-119-mudou-a-protecao-de-dados/>. Acesso em: 25 jun. 2023.

CARDOSO, C. **Como a TI sobreviveu aos ataques de 11 de Setembro**. Disponível em: <https://meiobit.com/446320/como-a-ti-sobreviveu-aos-ataques-de-11-de-setembro/>. Acesso em: 25 jun. 2023.

**Ataques de 11 de setembro ainda preocupam empresas americanas**. Disponível em: <https://valor.globo.com/carreira/noticia/2011/09/09/ataques-de-11-de-setembro-ainda-preocupam-empresas-americanas.ghtml>. Acesso em: 25 jun. 2023.‌

‌