Gestão de risco

Abordagem de conceitos de segurança da informação. Entendimento de fatores comprometedores dos ativos de informação de uma organização. Ações para diminuição de incidentes causadores de impactos indesejados no negócio.

Prof. Fabio Henrique Silva

Propósito

Esclarecer o funcionamento dos processos da gestão de risco para a quantificação e qualificação dos riscos associados à segurança da informação com base na norma ISO/IEC 27005 (parte integrante das normas da família ISO/IEC 27000).

Objetivos

- Definir vulnerabilidades, ameaças, ataques e termos relacionados à preservação da confidencialidade, integridade e disponibilidade (CID).
- Identificar as etapas da gestão de riscos (GR) de segurança da informação.

Introdução

Você já ouviu falar em segurança da informação?

Atualmente, há cada vez mais informações valiosas disponíveis no computador e na internet. Por isso, a cada dia que passa, surgem novas e mais elaboradas formas de ameaça à segurança da informação – e elas estão mais perto de nós do que imaginamos.

Alguns elementos associados à segurança da informação são: vulnerabilidades (pontos fracos), ameaças (como vírus e cavalos de Troia), riscos (a chance de um ataque ocorrer e um dano ser causado).

Compreender esses elementos é fundamental para que qualquer usuário aprenda a se proteger. Obter tal conhecimento se revela ainda mais importante para os estudantes de computação.

Assim sendo, percebemos a importância do estudo sobre os elementos associados à segurança da informação para os envolvidos em gestão de dados e áreas afins.

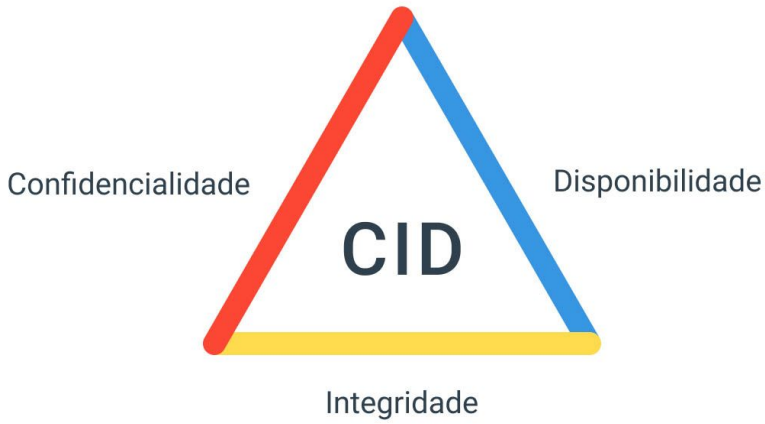
Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Segurança da informação

Pilares

Para identificarmos a quais riscos um ativo de informação pode estar submetido, precisaremos, antes disso, estudar alguns termos e conceitos relacionados à preservação dos seguintes pilares da segurança da informação:



No CID, minimiza-se o risco da ocorrência de incidentes de:

Confidencialidade

Que disponibilizem uma informação para pessoas, entidades ou processos não autorizados.

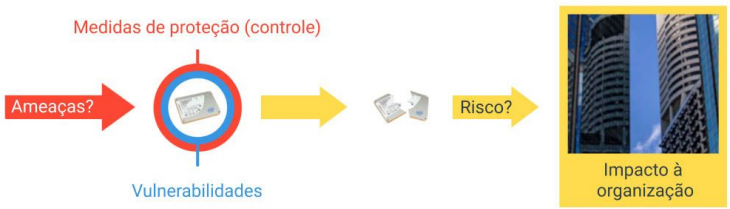
Integridade

Que afetem a exatidão e a integralidade de ativos.

Disponibilidade

Que tornem os recursos inacessíveis e inutilizáveis sob demanda.

Esmiuçaremos todos os elementos a seguir:



Ativos

Toda empresa possui seus ativos, ou seja, algo que possui valor para a organização. Exibiremos a seguir alguns de seus exemplos:

1. **Ativos de informação:** Base de dados, arquivos, contratos e acordos.
2. **Ativos de software:** Aplicativos e sistemas.
3. **Ativos físicos:** Equipamentos computacionais e de comunicação.
4. **Serviços:** Eletricidade e refrigeração.
5. **Pessoas:** Suas qualificações, habilidades e experiências.
6. **Intangíveis:** Aqueles que não podemos tocar, como a reputação e a imagem da organização.

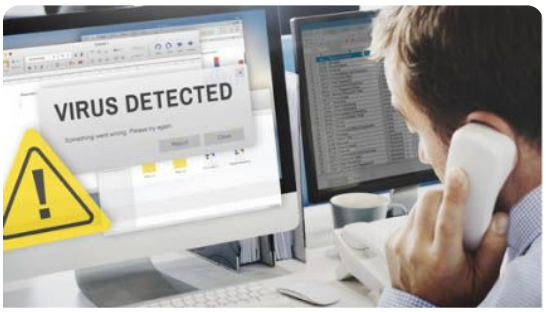
Ameaças

Em seu item 3.74, a norma ISO/IEC 27000:2018 define ameaça como “a causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização por meio da quebra de segurança”.

Nenhuma organização deseja que qualquer tipo de ativo sofra algum dano ou furto. No entanto, justamente pelo fato de possuírem uma percepção de valor, os ativos estão sujeitos a ameaças de várias naturezas. Elas podem ser:

Físicas

Falhas de equipamentos e instalações, como relâmpagos, terremotos, ataques a bombas, deterioração dos meios de armazenamento, fraude, roubo, invasão etc.



Lógicas

Vulnerabilidades em softwares, como bugs, vírus, malwares etc.

Note que o contrário de ameaça é oportunidade, cujo significado é: “Ocasião favorável; circunstância oportuna e propícia para a realização de alguma coisa; ensejo” (MICHAELIS, 2020, n. p.).

Podemos então reescrever o conceito de oportunidade como a causa potencial de um incidente desejado que pode resultar em ganho para um sistema ou uma organização.

Medidas de proteção (controle)

Certas ameaças rondam os ativos a todo instante.

Como uma organização deseja mantê-los a salvo, deve adotar medidas de proteção (controle) para esconder ou diminuir o acesso ou a exposição às vulnerabilidades deles.

Segundo o item 3.14 da norma ISO/IEC 27000:2018, **controle** é uma medida que pode modificar o risco por meio de processo, política, dispositivo, prática ou outras ações que modifiquem a ameaça e/ou a vulnerabilidade e, consequentemente, o risco.

Vulnerabilidades

A vulnerabilidade "é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças e, por consequência, comprometer a segurança de sistemas ou informações". A identificação dela em um ativo, porém, não é um processo trivial.

Desse modo, deve-se inicialmente realizar uma **análise de vulnerabilidades**, que é o processo de levantar falhas ou ausências em um conjunto de proteções adotadas. Em seguida, a **avaliação de vulnerabilidades** é feita com uma lista de ameaças no intuito de avaliar sua probabilidade de ocorrência.

A tabela a seguir apresenta alguns exemplos de ameaças, vulnerabilidades e medidas de controle cabíveis:

Ameaças	Vulnerabilidades	Medidas de controle
Lógicas	• Problemas no sistema operacional; • Falhas em aplicativos; • Sites perigosos da web.	• Instalação de antivírus; • Firewall; • Lista de controle de acesso; • Atualização do sistema operacional.
Físicas	• Falta de identificação de visitantes na empresa; • Fios soltos; • Sala do datacenter acessível para qualquer pessoa.	• Instalação de câmeras de segurança; • Acesso à sala por controle biométrico; • Piso elevado contra enchentes; • Para-raios; • Nobreaks.

Ameaças, vulnerabilidades e medidas de controle.
Tabela: Fabio Henrique Silva

Incidente

Nenhuma medida de proteção é infalível. Portanto, uma ameaça pode explorar uma ou mais vulnerabilidades não cobertas pelas medidas de proteção adotadas. Quando uma delas ocorre, há um **incidente de segurança da informação**.

Exemplo

A instalação de um malware, o roubo de senhas ou um usuário conseguir copiar dados não autorizados com seu pen drive.

O conceito de incidente de segurança da informação é definido pelo item 3.31 da norma ISO/IEC 27000:2018 como um “evento ou série de eventos indesejados ou inesperados que provavelmente comprometerão as operações da empresa ou ameaçam a segurança da informação”.

Evento

Um evento de segurança da informação não implica necessariamente um incidente de segurança da informação. Com base no item 3.30 da norma ISO/IEC 27000:2018, um **evento de segurança da informação** significa uma “ocorrência identificada de um estado de rede, serviço ou sistema que indique uma possível falha da política de segurança ou falha das salvaguardas, ou mesmo uma situação até então desconhecida que pode se tornar relevante em termos de segurança”.

Exemplo

O travamento não esperado de uma aplicação ou uma pessoa que acidentalmente desconecta um cabo.

Vamos entender melhor a seguir a diferença entre impacto e risco.

Impacto

Já sabemos que uma ameaça explora vulnerabilidade(s) de um ativo e causa um incidente de segurança da informação. Tal incidente, por sua vez, pode gerar um impacto na organização. Segundo a norma ISO/IEC 27000:2018, “ele é caracterizado como uma mudança não desejável nos objetivos de negócios”.

Risco

É caracterizado no item 3.61 da norma ISO/IEC 27000:2018 como a combinação das consequências de um evento (incluindo mudanças nas circunstâncias) e de sua probabilidade associada de ocorrência.

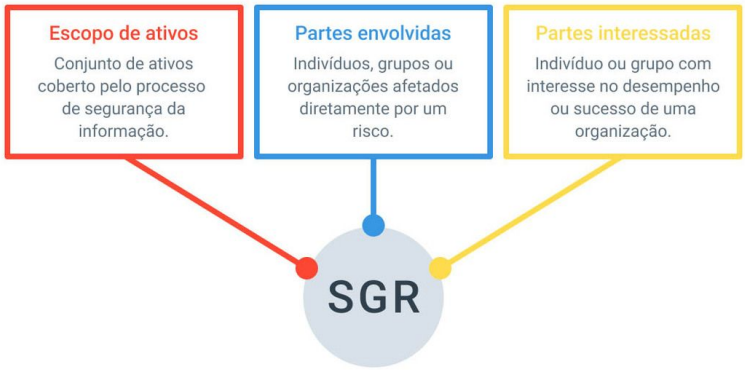
Sistemas de gestão

Sistemas de gestão de riscos (SGR)

Você já ouviu falar em SGR?

Trata-se do conjunto de práticas e procedimentos utilizado para gerenciar os riscos.

Tanto a ocorrência de um incidente de segurança da informação quanto o impacto causado por seu incidente poderão ser minimizados se uma organização adotar um SGR. Sua aplicação é importante a fim de diminuir possíveis danos e prejuízos causados por eventuais incidentes. Vejamos!



Sistema de Gestão de Segurança da Informação (SGSI)

De acordo com a norma ABNT NBR ISO/IEC 27001, o processo de gestão de riscos de segurança da informação deve atender aos requisitos de um SGSI. Confira um pouco mais sobre o SGSI.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

Para encerrarmos essa etapa de aprendizado, apresentaremos um resumo dos termos e das definições relacionadas à segurança da informação.

1. Controle: (ISO/IEC 27000:2018, item 3.14) - Medida que pode modificar o risco por meio de um processo, política, dispositivo, prática ou outras ações que modifiquem a ameaça e/ou a vulnerabilidade – e, consequentemente, o risco.

2. Ameaça: (ISO/IEC 27000:2018, item 3.74) - Causa potencial de um incidente indesejado, podendo resultar em dano para um sistema ou uma organização por meio da quebra de segurança.

3. Vulnerabilidade: (ISO/IEC 27000:2018, item 3.77) - Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças e, por consequência, comprometer a segurança de sistemas ou informações.

4. Análise de vulnerabilidades: Processo de levantar falhas ou ausências em um conjunto de proteções.

5. Avaliação de vulnerabilidades: Combinação da análise e de uma lista de ameaças para avaliar a probabilidade de elas ocorrerem.

6 Evento de segurança da informação: (ISO/IEC 27000:2018, item 3.30) - Ocorrência identificada de um estado de rede, serviço ou sistema que indique uma possível falha da política de segurança ou das salvaguardas, ou mesmo uma situação até então desconhecida que pode se tornar relevante em termos de segurança.

7. Incidente de segurança da informação:(ISO/IEC 27000:2018, item 3.31) - Evento ou série de eventos indesejados ou inesperados que provavelmente compromete as operações da empresa ou ameaça a segurança da informação.

8. Risco: (ISO/IEC 27000:2018, item 3.61) - Combinação das consequências de um evento (incluindo mudanças nas circunstâncias) e de sua probabilidade associada de ocorrência.

9. Impacto: Mudança não desejável nos objetivos de negócios.

10. Escopo de ativos: Define o conjunto de ativos coberto pelo processo.

11. Parte envolvida: Indivíduos, grupos ou organizações afetados diretamente por um risco.

12. Parte interessada: Indivíduo ou grupo com interesse no desempenho ou sucesso de uma organização.

Vem que eu te explico!

Os vídeos a seguir abordam os assuntos mais relevantes do conteúdo que você acabou de estudar.

Sistemas de Gestão de Riscos

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Controle e Prevenção de Ameaças

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Análise e Avaliação de Vulnerabilidades em SGSI

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Imagine que uma pessoa não autorizada conseguiu invadir o datacenter de uma organização corporativa que possui roteadores e servidores. Dentro dos termos relacionados à segurança da informação, esta pessoa, para a corporação, pode ser considerada:

A

Impacto

B

Vulnerabilidade

C

Controle

D

Ameaça

E

Stakeholder

A alternativa D está correta.

A norma ABNT NBR ISO/IEC "27002":2013 diz que "ativos são objeto de ameaças tanto acidentais como deliberadas. [...] em função das várias maneiras nas quais as ameaças podem se aproveitar das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz esses riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos".

Questão 2

Segundo a norma ABNT NBR ISO/IEC "27001":2013, uma organização, para entender as necessidades e as expectativas das partes interessadas, “deve "determinar": a) As partes interessadas que são relevantes para o sistema de gestão de segurança da informação; e b) Os requisitos dessas partes interessadas relevantes para a segurança da informação”.

As partes interessadas em um sistema de gestão de segurança da informação podem ser entendidas como:

A

As pessoas que não possuem interesse na organização.

B

Os indivíduos ou grupos que se interessam pelo desempenho ou sucesso da organização.

C

Pessoas que possuem interesses estritamente pessoais.

D

Outras empresas que realizam as próprias análises de risco.

E

Indivíduos promotores dos eventos de risco.

A alternativa B está correta.

As partes interessadas são pessoas, grupos ou organizações que podem gerar um impacto ou ser impactados pelo desempenho da organização.

Risco à segurança da informação

Antes de conhecê-los, precisamos entender como são realizados os processos da gestão de riscos (GR) dentro da Gestão de Segurança da Informação (GSI). Para isso, analisaremos um exemplo.

A organização XPTO possui um servidor que executa um banco de dados com os seguintes elementos:

- **Escopo de ativos:** Servidor e banco de dados.
- **Vulnerabilidades identificadas:** Falha no software que pode ser explorada devido a outra no sistema operacional.
- **Ameaça:** Malware codificado para explorar as vulnerabilidades citadas e roubar dados do banco de dados.
- **Medida de controle adotada:** Instalação de suíte de antivírus.
- **Medidas de controle não adotadas:** Atualização de sistema operacional e software.
- **Possível incidente de segurança da informação:** Malware chega por e-mail para um usuário, que executa o arquivo anexado.
- **Impactos:** Roubo de dados sensíveis e prejuízo financeiro.
- **Risco:** Risco extremo.

Um *malware* chamado *No pain, no gain* está causando pânico nas empresas ao redor do mundo justamente por explorar as vulnerabilidades identificadas nelas e roubar seus dados sensíveis. Existe, portanto, uma alta probabilidade de esse malware explorar tais vulnerabilidades, caso as medidas de controle restantes não sejam adotadas, causando, com isso, um impacto grave nos negócios dessas organizações. Para a XPTO, esse risco é relevante e foi classificado como risco extremo.

> Neste caso, que medidas devem ser tomadas?

O plano de tratamento definido, nesse caso, foi o seguinte: evitar a ocorrência do incidente de forma preventiva, instalando as atualizações de software necessárias. Para isso, deve ser realizada uma comunicação às partes envolvidas antes e depois das atualizações. Após a aplicação delas, o risco será monitorado para prever a ocorrência de outras possíveis vulnerabilidades.

Cada organização percebe os riscos de forma diferente. Neste exemplo, a organização Ajax (concorrente da XPTO) realizou uma **percepção de risco** diferente da empresa XPTO. Ela utiliza outro tipo de sistema operacional e outro tipo de software de banco de dados, que não são afetados pelo malware *No pain no gain*. Logo, dentro de seu atual contexto, esse malware pode não fazer parte da percepção de risco.

Uma vez percebido, um risco passa pelo crivo de tolerância, determinando se ele será tratado ou não.

> O nome desse processo é critério de risco (o que a organização define como tolerável).

Os que sobram após o tratamento são chamados de riscos residuais: trata-se daqueles considerados pequenos ou que, apesar das respostas não implementáveis, devem ser monitorados.

Gestão de riscos

As seguintes normas relacionadas à gestão de riscos (GR) podem ser levadas em consideração pelos profissionais da segurança da informação:

- **ABNT NBR ISO/IEC 27005** - Gestão de riscos de segurança da informação
- **ABNT NBR ISO/IEC 31000** - Gestão de riscos – princípio de diretrizes

Com elas, é possível entender o conceito, o funcionamento e as etapas de uma GR.

Mas, afinal, qual é o papel da GR?

Conceito

A gestão de riscos é o processo que identifica e trata os riscos de forma sistemática e contínua. Trata-se de um dos componentes mais importantes da GSI.

Funcionamento

Para ter sucesso, a GR deve ser permanente, mostrando-se capaz de identificar novas vulnerabilidades e ameaças que podem afetar os três pilares de segurança da informação: confidencialidade, integridade e disponibilidade (CID).

Mas fique atento a alguns detalhes importantes.

Atenção

É necessário criar uma estrutura adequada para essa gestão. Dessa forma, tão importante quanto a definição de funções e responsabilidades é o desenvolvimento de uma cultura de GR. Com isso, uma organização mantém seu nível de risco em patamares aceitáveis.

Etapas da gestão de riscos

A GR compreende as seguintes etapas:

Definição do contexto

Inicialmente, deve-se fazer a listagem e um breve resumo dos objetivos organizacionais, pois, se seus riscos não forem atingidos, eles terão de ser gerenciados. Dessa forma, é feito um levantamento de informações relevantes sobre o ambiente no qual será executada a análise de riscos.

Deve estar claro nesse levantamento o entendimento sobre as atividades da organização e os propósitos que a levaram à GSI, como suporte ao SGSI, conformidade legal, plano de continuidade de negócios e de resposta a incidentes (BEZERRA, 2013).

Bezerra (2013) ainda elenca os itens que devem constar nessa análise da organização:

Itens da análise da organização

- Propósito principal da organização
- Negócio
- Missão
- Visão de futuro
- Valores
- Estrutura organizacional
- Organograma
- Estratégias
- Produtos
- Parceiros
- Terceiros
- Instalações
- Funcionários

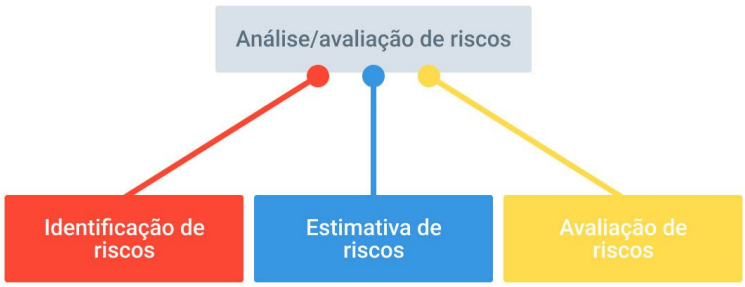
Por fim, são estabelecidos **parâmetros** para o gerenciamento dos riscos.

Parâmetros

Escalas de probabilidade e impacto, definição do apetite a risco e nível de risco considerado aceitável.

Processo de análise/avaliação de riscos de segurança da informação

Esta etapa se divide em:



A análise/avaliação de riscos consiste nas seguintes atividades: Análise de riscos (Seção 8.2) compreende: - Identificação dos riscos (Seção 8.2.1); - Estimativa dos riscos (Seção 8.2.2); - Avaliação de riscos (Seção 8.3).

A **identificação de riscos** mapeia os eventos de risco que podem impedir uma empresa de atingir os objetivos desejados. A análise de riscos, por sua vez, compreende a identificação e a estimativa deles.

Pode-se começar com uma lista dos eventos de risco associados aos objetivos institucionais, evoluindo, em seguida, para um nível maior de detalhamento. Após realizar o mapeamento e a relação desses eventos, listam-se as suas possíveis causas e consequências de cada um deles.

Já a **estimativa de riscos** mede os eventos de risco por meio do cálculo do nível de risco. Deve-se iniciar tal

processo realizando o cálculo do nível de risco bruto.

Para isso, são avaliados a probabilidade e o impacto de um evento de risco antes que uma medida de controle qualquer seja implementada, conforme os exemplos das duas tabelas a seguir:

Probabilidade	Termo	Definição
71 a 90%	Alta	Chance de a ameaça se concretizar em um ano
31 a 70%	Média	Possibilidade de a ameaça se concretizar no próximo ano
1 a 30%	Baixa	Dificilmente a ameaça ocorrerá no próximo ano

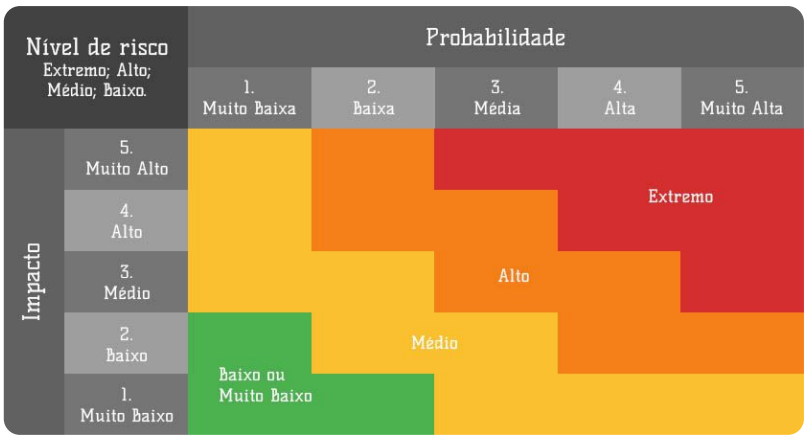
Medição qualitativa da probabilidade – exemplificação. Probabilidade: chance de um evento acontecer.Tabela: Peltier, 2005, p. 173

Impacto	
Termo	Definição
Alto	Grave comprometimento da missão da organização
Médio	As perdas são restritivas a um segmento dela
Baixo	Sem muita relevância para seus negócios

Medição qualitativa da probabilidade – exemplificação. Impacto: medida para avaliar a magnitude de uma eventual perda.Tabela: Peltier, 2005, p. 173)

Em seguida, é **avaliada a qualidade** das medidas de controle que existem para impedir o risco bruto. Obtém-se, com isso, o risco residual, ou seja, o que sobra do bruto depois de ele ser mitigado pela atividade de controle.

Monta-se uma tabela em ordem decrescente em relação ao nível de risco residual para verificar os eventos de risco que devem ser tratados com prioridade. Para cada risco considerado prioritário, elabora-se uma matriz de impacto versus probabilidade. Observemos esta tabela:



Matriz de riscos.Tabela: Brasil, 2019.

A avaliação de riscos, por sua vez, define as medidas de tratamento a serem implementadas para cada um dos eventos de risco, entre as quais destacamos:

Ao lado de cada evento de risco, deve ser informada a forma de tratamento a ser adotada. Isso é feito tendo como base o nível de risco residual e o apetite a risco identificado na definição do contexto.

Tratamento do risco de segurança da informação

Esta etapa estabelece como cada opção de tratamento é implementada.

Exemplo

Caso um evento de risco seja deliberado para ser mitigado, é necessária a indicação, entre outros itens, da medida de controle responsável por fazer essa mitigação, do seu prazo e de quem é o responsável por implementá-la.

Toda medida de tratamento deve conter a indicação dos responsáveis por sua implementação – no caso, os gestores do risco. No tratamento do risco, são selecionadas e implementadas medidas de forma a reduzir os riscos identificados. Desse modo, o plano de tratamento do risco (PTR) é definido. A seguir, são feitas recomendações para que a empresa crie ou modifique os mecanismos de segurança existentes.

Para cada forma de ameaça, deve ser definida uma ou mais medidas de proteção (controles). Tais medidas precisam ser aplicadas nos ativos, além de seus custos. Um exemplo disso é o uso de criptografia e senha robusta.

Os resultados serão as respostas às seguintes questões:

1. O que deve ser protegido?
2. A que custo?
3. De quem proteger?
4. Com que riscos?

No custo desejado, a proteção provavelmente não dará uma segurança total.

Medidas de controle ou proteção

As medidas de controle ou proteção podem ser classificadas como:

- **Preventiva:** Evita que incidentes ocorram.
- **Desencorajadora:** Desencoraja a prática de ações.
- **Monitoradora:** Monitora o estado e o funcionamento.

- **Corretiva:** Corrige falhas existentes.
- **Recuperadora:** Repara danos causados por incidentes.
- **Reativa:** Reage a determinados incidentes.
- **Detectora:** Detecta a ocorrência de incidentes.
- **Limitadora:** Diminui os danos causados.

Aceitação do risco de segurança da informação

A decisão de aceitar os riscos residuais não basta: é necessário se responsabilizar por ela. Afinal, é responsabilidade da política de gestão de riscos oferecer suporte a essa tomada de decisão.

Comunicação do risco de segurança da informação

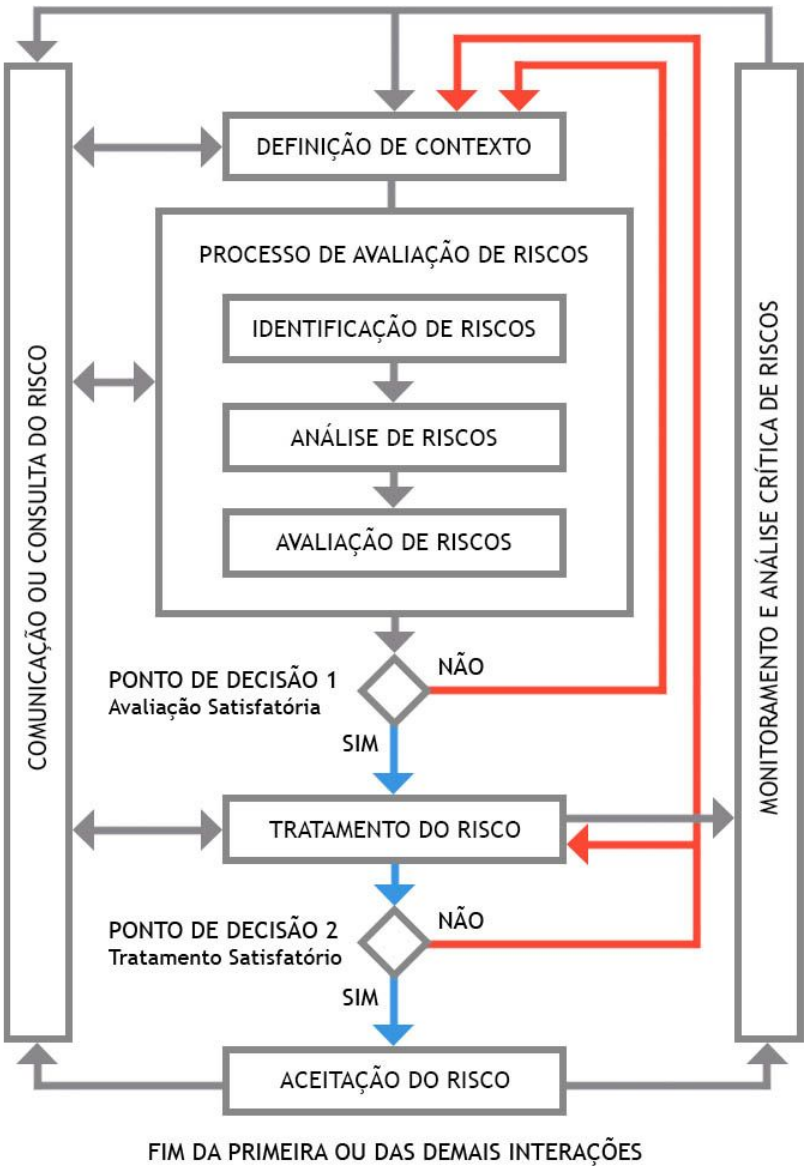
Recomenda-se que as informações sobre riscos sejam trocadas ou compartilhadas entre o tomador de decisão e as outras partes interessadas para haver um consenso sobre como eles devem ser administrados.

Monitoramento e análise crítica de riscos de segurança da informação

Nesta etapa, é avaliado se tudo o que foi feito saiu de acordo com o planejado. Além disso, são averiguados, dentre outros, os seguintes casos:

- Necessidade de atualizações.
- Listagem correta dos objetivos.
- Impossibilidade de um risco ser visto como esperado pelas atividades de controle.
- Cálculo correto dos níveis de risco.

A imagem a seguir ilustra uma visão do processo de gestão de risco (GR) segundo a norma ABNT NBR ISO/IEC 27005:



Processo de GR

Governança, risco e compliance

A GR compõe alguma ferramenta utilizada no mundo dos negócios? Como obter maiores vantagens competitivas no âmbito da gestão?

Faremos agora algumas considerações que esclarecem tais questões.

A GR compõe uma ferramenta cada vez mais utilizada no mundo dos negócios: **Governança, Riscos e *Compliance* (GRC)**. A organização que tiver a GRC como parte de suas diretrizes estará mais preparada para obter maiores e melhores vantagens competitivas.

Qual é o papel da GRC neste cenário?

Governança corporativa

Cuida para que o controle da gestão seja tão importante quanto ela própria.

Gestão de riscos

Gerencia o efeito da incerteza nos objetivos.

Compliance

Adere aos padrões da legislação (regulamentos oficiais vigentes, políticas empresariais e normas internas de procedimentos)

Para compreendermos melhor a aplicação desses conceitos, analisaremos o caso a seguir:

Exemplo

Uma empresa do ramo de energia possui um departamento de TI que realiza operações gerenciadas e suportadas pela GRC. Por meio de entrevistas semiestruturadas, foi realizada uma análise dos esforços de integração da GRC de TI com base em um modelo com cinco dimensões, que serão aqui representadas pelos seguintes termos: 1. G-TI: Nível de maturidade da governança de TI 2. gR-TI: Nível de maturidade do gerenciamento de riscos de TI 3. C-TI: Nível de maturidade do processo de conformidade de TI 4. GRC-TI: Grau de integração entre G-TI, gR-TI e GRC-TI 5. GRC/GRC-TI: Grau de integração entre a GRC corporativa e a GRC da TI Todas as dimensões podem ter um dos três valores possíveis que representam o nível de maturidade de seus processos: alto, médio e baixo. Para cada uma das três disciplinas (GRC), verificou-se se os quatro componentes a seguir eram integrados e aplicados holisticamente em toda a organização: estratégia, processos, pessoas e tecnologia.

Nesse contexto, foram encontrados os seguintes resultados:

G-TI: Nível de maturidade da governança de TI

A empresa concentra-se em três entregas da G-TI: maturidade dos serviços prestados, satisfação do parceiro de negócios e eficácia do gerenciamento de projetos. Ela usa a governança para “abordar o comportamento correto para alcançar as metas corporativas”.

Garante alinhamento e contribuição para o valor comercial um triângulo do CIO (sigla de *chief information officer* ou, em português, gerente de TI). Ele representa os interesses de TI do grupo, o fornecedor interno de serviços e projetos de TI e as operações de negócios que definem a demanda de TI.

O CIO é responsável por todas as facetas do G-TI, compartilhando responsabilidades e tarefas de suporte com os líderes de TI da unidade de negócios e líderes de divisão, além de envolver vários comitês.

Para uma perspectiva em que a governança é claramente formalizada, mesmo se concentrando mais em responsabilidades e objetivos, e centrada no CIO, o grau de maturidade pode ser definido como "alto".

gR-TI: Nível de maturidade do gerenciamento de riscos de TI

O processo gR-TI normalmente começa com uma fase de planejamento na qual os objetivos de risco são definidos.

A identificação e a avaliação de riscos são realizadas antes que as medidas de resposta a eles sejam selecionadas e implementadas. Os riscos são monitorados e relatados às partes interessadas relevantes.

A empresa utiliza um produto de software para a implementação do gR-TI que lembra a metodologia ISO 270005. O software não usa probabilidades, baseando-se na comparação dos impactos reais com os valores-alvo.

O gR-TI apresenta alta maturidade ("alto").

C-TI: Nível de maturidade do processo de conformidade de TI

A empresa não possui um processo C-TI independente definido, pois as atividades do C-TI são integradas ao gR-TI. Essas atividades integradas evoluem em torno dos padrões da linha ISO/IEC 27000 e de outros padrões.

O escritório do CIO realiza auditorias de TI constantemente. Existe um software que suporta o gerenciamento de conformidade, enquanto os aplicativos de outros fornecedores garantem prevenção, monitoramento e detecção de conformidade. Um outro aplicativo permite gerenciar suas políticas de controle de acesso e autorização.

Pode-se avaliar que a maturidade é "média" devido à menor formalização.

GRC-TI: Grau de integração entre G-TI, gR-TI e GRC-TI

No nível do processo, a integração do C-TI ao gR-TI está muito avançada, sendo o C-TI realizado como parte do gR-TI.

A empresa implantou um software para gerenciamento de conformidade, enquanto os aplicativos de vários outros fornecedores garantem prevenção, monitoramento e detecção de conformidade. Existe um aplicativo para gerenciar controles de acesso e autorização, mas, por ser mais uma ferramenta operacional, ele não está no escopo do gerenciamento de GRC-TI.

A ferramenta de gerenciamento de riscos ajudou a padronizar o gR-TI, porém as soluções automatizadas adicionais de controle e monitoramento estão desconectadas. Embora a empresa não dependa de planilhas, suas atividades de gerenciamento de GRC de TI não são suportadas por uma solução abrangente.

A maturidade da integração pode ser descrita como "média", pois pode-se observar a integração principalmente nos níveis de processo e de pessoal, ainda que a integração da tecnologia fique para trás.

GRC/GRC-TI: Grau de integração entre a GRC corporativa e a GRC da TI

Na empresa, a governança corporativa influenciou na criação de seu modelo G-TI, assim como o papel do CIO na governança corporativa também o vincula ao G-TI. A empresa usa aplicativos de software para gerenciamento estratégico de riscos.

Diferentes processos (com atividades semelhantes) são usados para realizar o gR-TI e o gerenciamento de riscos corporativo.

A C-TI está conectada à conformidade corporativa de várias maneiras. Apenas uma parte da infinidade de requisitos de GRC é direcionada para operações de TI. Assim, os processos devem ser examinados de ponta a ponta.

A empresa não possui uma ferramenta central que armazena todos os dados relevantes à conformidade (normas, resultados de auditoria, registros, informações de controle etc.).

Devido à baixa automação do processo, a maturidade é classificada como "média".

Pra finalizar nosso assunto, vamos saber um pouco mais no video a seguir.

Processo de gestão de risco e exemplo de matriz de risco

Confira agora os meandros do processo de gestão de risco e alguns exemplos para contribuir com sua análise.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Vem que eu te explico!

Os vídeos a seguir abordam os assuntos mais relevantes do conteúdo que você acabou de estudar.

Riscos à Segurança da Informação

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Etapas da Gestão de Riscos

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Governança, Riscos e Compliance

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Segundo a ABNT (2018), a avaliação de riscos de TI e segurança da informação é baseada na elaboração da uma matriz de risco estruturada com aderência à norma ISO/IEC 27005. Tal norma identifica os principais itens que compõem o ambiente avaliado, especificando com clareza suas vulnerabilidades e ameaças.

Além disso, a matriz apresenta o impacto da exploração dessas vulnerabilidades pelas ameaças e a probabilidade de tal ocorrência. O risco, portanto, é um resultado da função impacto versus probabilidade, sendo estimado quantitativa (estimativa numérica) e qualitativamente (conceitual).

Analise as afirmativas a seguir:

I - Uma vez que uma ameaça explora vulnerabilidade(s) de um ativo e causa um incidente de segurança da informação, este, por sua vez, poderá causar um impacto não desejável à organização, ou seja, uma mudança não desejável nos objetivos de negócios.
II - Se uma organização adotar o conjunto mais econômico de medidas para controlar os riscos, pode-se afirmar com toda a certeza que ela pode dispensar a utilização das etapas da gerência de riscos, pois toda a organização irá obter o nível de risco no patamar "inexistente".
III - Uma típica matriz de risco consegue apresentar graus para a medição qualitativa ou quantitativa da probabilidade, mas fica inviável apresentar graus para a medição do impacto.

Marque a alternativa que possui somente as afirmativas verdadeiras:

A

Somente II.

B

Somente I.

C

I e III.

D

I, II e III.

E

I e II.

A alternativa B está correta.

A Gerência de Riscos (GR) deve ser permanente, pois sempre podem existir vulnerabilidades e ameaças que podem afetar os pilares de segurança da informação. A adoção permanente de uma cultura de Gestão de Riscos pode manter o nível dos riscos em patamares aceitáveis. Em uma GR, as Matrizes de Riscos serão elaboradas, utilizadas e melhoradas continuamente. Uma típica matriz de riscos apresenta os possíveis graus de riscos, decorrentes das escalas de medição qualitativa e/ou quantitativa da probabilidade e do impacto.

Questão 2

A tabela a seguir oferece um resumo dos tipos de ameaças à segurança enfrentadas no uso da web:

	AMEAÇAS	CONSEQUÊNCIAS
Integridade	• Modificação de dados do usuário; • Navegador cavalo de troia; • Modificação de memória • Modificação de tráfego de mensagem em trânsito.	• Perda de informações; • Comprometimento da máquina; • Vulnerabilidade a todas as outras ameaças.
Confidencialidade	• Espionagem na rede; • Roubo de informações do servidor; • Roubo de dados do cliente; • Informações sobre configuração de rede; • Informações sobre qual cliente fala com o servidor.	• Perda de informações; • Perda de privacidade.

	AMEAÇAS	CONSEQUÊNCIAS
Negação de serviço	• Encerramento de processos do usuário; • Inundação da máquina com solicitações falsas; • Preenchimento do disco ou da memória; • Isolamento da máquina por ataques de domain name system (DNS).	• Interrupção; • Incômodo; • Impede que o usuário realize o trabalho.
Autenticação	• Personificação de usuários legítimos; • Falsificação de dados.	

Tabela: STALLINGS, 2015, p. 412

Mostramos acima um levantamento das consequências de algumas ameaças para um grupo de aspectos de segurança. Na gestão de riscos, este tipo de tabela, sem levar em consideração a tomada de decisão feita após sua elaboração, pode ser um dos frutos da atividade da seguinte etapa:

A

Estabelecimento do contexto.

B

Análise dos riscos.

C

Tratamento do risco.

D

Aceitação do risco residual.

E

Matriz de probalidade *versus* impacto.

A alternativa B está correta.

A análise ou estimativa de riscos faz parte da etapa de processo de avaliação deles. Os objetivos desta etapa são identificar os riscos e definir o que deve ser feito para diminui-los até um nível aceitável. Esta tabela mostra o levantamento realizado na etapa de identificação deles. Após isso, é possível realizar sua estimativa e avaliação.

Considerações finais

A preservação da segurança da informação dos ativos de uma organização passa pelas etapas da GR, a qual, por sua vez, atua dentro do escopo de GRC.

Essas etapas oferecem ferramentas para a identificação de ameaças e a adoção de controles. Seu objetivo, afinal, é minimizar, para as partes envolvidas e interessadas, o impacto causado por um incidente.

Podcast

A seguir ouça um resumo do que vimos até aqui.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore +

Confira as indicações que separamos especialmente para você!

Leia a seguinte cartilha:

BRASIL. Agência Nacional de Saúde Suplementar. **Política de gestão de riscos**. Risco: efeito de incertezas nos objetivos. Brasília: ANS, 2009.

Busque e assista às seguintes conferências TED:

TEDxMileHigh - Risk management ou gerenciamento de riscos (2012), com Chris Davenport, um famoso alpinista.

TEDxYYC - Três ferramentas simples, divertidas e eficazes para ajudar a gerenciar riscos (2016), com Will Gadd, escritor, cineasta e famoso atleta de aventura ao ar livre.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT. ABNT NBR ISO/IEC 27000:2018**. Tecnologia da informação — técnicas de segurança — sistemas de gerenciamento de segurança da informação – visão geral e vocabulário. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. **ABNT NBR ISO/IEC 27005:2019**. Tecnologia da informação — técnicas de segurança — gestão de riscos de segurança da informação. 2019.

BEZERRA, E. K. **Gestão de riscos de TI**: NBR 27005. Rio de Janeiro: RNP/ESR, 2013.

BRASIL. **Resolução nº 603, de 29 de outubro de 2019**. Ementa: Aprova o plano de gestão de riscos do Conselho Regional de Contabilidade do Rio Grande do Sul. DOU. ed. 217. seção 1. p. 239. Publicado em: 8 nov. 2019.

CEFET JR. **Quatro dicas para criar uma análise SWOT**. Publicado em: 6 jan. 2019.

MICHAELIS. **A mais completa linha de dicionários do Brasil**. Consultado na internet em: 24 mar. 2020.

PELTIER, T. R. *Information security risk analysis*. Boca Raton: Auerbach Publications, 2005.

PORTAL ISO 27000. **Análise de riscos de TI**. Consultado na internet em: 24 mar. 2020.

RACZ, N.; WEIPPL, E.; BONAZZI, R. ***IT governance, risk & compliance (GRC) status quo and integration**: an explorative industry case study. ResearchGate, jul. 2011*.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.