UNIP
UNIVERSIDADE PAULISTA
Interativa

Segurança da Informação

Autor: Prof. Ricardo Sewaybriker
Colaboradores: Prof. Roberto Macias
Profa. Elisângela Mônaco de Moraes
Prof. Fábio Vieira do Amaral

Professora conteudista: Ricardo Sewaybriker

Pós-graduado em Gestão de Segurança da Informação pelo Instituto de Pesquisa Energéticas e Nucleares (IPEN) – USP, Ricardo Sewaybriker é administrador profissional formado em Administração de Empresas pelas Faculdades Integradas Campos Salles (FICS), professor líder da disciplina presencial de Segurança da Informação na UNIP e profissional de segurança da informação, atuando em instituição financeira há 21 anos.

Atua como professor orientador de diversos projetos integrados multidisciplinares dos cursos presenciais de Tecnologia da Informação e de trabalhos de conclusão do curso presencial de Administração de Empresas da UNIP.

Dados Internacionais de Catalogação na Publicação (CIP)

S514s Sewaybriker, Ricardo

Segurança da informação / Ricardo Sewaybriker. 2. ed. São Paulo: Editora Sol, 2020.

176 p., il.

1. Segurança da informação. 2. Gestão de risco. 3. Auditoria de Sistemas. I.Título.

CDU 65.011.56

U410.95 – 20

© Todos os direitos reservados. Nenhuma parte desta obra pode ser reproduzida ou transmitida por qualquer forma e/ou quaisquer meios (eletrônico, incluindo fotocópia e gravação) ou arquivada em qualquer sistema ou banco de dados sem permissão escrita da Universidade Paulista.

Prof. Dr. João Carlos Di Genio
Reitor

Prof. Fábio Romeu de Carvalho
Vice-Reitor de Planejamento, Administração e Finanças

Profa. Melânia Dalla Torre
Vice-Reitora de Unidades Universitárias

Prof. Dr. Yugo Okida
Vice-Reitor de Pós-Graduação e Pesquisa

Profa. Dra. Marília Ancona-Lopez
Vice-Reitora de Graduação

Unip Interativa – EaD

Profa. Elisabete Brihy
Prof. Marcelo Souza
Prof. Dr. Luiz Felipe Scabar
Prof. Ivan Daliberto Frugoli

Material Didático – EaD

Comissão editorial:
Dra. Angélica L. Carlini (UNIP)
Dra. Divane Alves da Silva (UNIP)
Dr. Ivan Dias da Motta (CESUMAR)
Dra. Kátia Mosorov Alonso (UFMT)
Dra. Valéria de Carvalho (UNIP)

Apoio:
Profa. Cláudia Regina Baptista – EaD
Profa. Betisa Malaman – Comissão de Qualificação e Avaliação de Cursos

Projeto gráfico:
Prof. Alexandre Ponzetto

Revisão:
Aileen Nakamura

Sumário

Segurança da Informação

Unidade III

Unidade IV

APRESENTAÇÃO

Olá, caros alunos!

Esta disciplina, Segurança da Informação, tem como objetivo abordar de forma simples e objetiva os fatores que cercam a proteção do ativo mais importante para uma organização: a informação.

O conteúdo que será apresentado visa à interação, ao envolvimento e ao despertar da curiosidade do aluno a partir desse importante tema que, apesar de antigo, se transforma e se renova a cada momento por causa das modificações tecnológicas e dos fraudadores que estão sempre desenvolvendo novas técnicas de invasão.

Diante desse cenário, veremos na Unidade I os princípios básicos de segurança da informação, como seu valor, vulnerabilidade, impacto e risco, além de passarmos pela noção de risco e de como analisá-lo e gerenciá-lo.

Na Unidade II, veremos os aspectos éticos e legais do uso tecnológico, como a educação e o direito digital, além das normas e padrões de segurança da informação, assim como o processo de auditoria de sistemas.

Já na Unidade III, passaremos pela segurança na autenticação, pelo controle de acesso e pelos aspectos tecnológicos da segurança da informação.

Finalmente, na Unidade IV, estudaremos os planos de continuidade de negócio e suas estratégias, as principais práticas em segurança da informação e o uso da criptografia, com seus mecanismos de proteção.

A importância em proteger os ativos de informação é latente para os profissionais de todas as áreas, afinal, vivemos na era da informação, em que o uso adequado auxilia os processos em todos os níveis da empresa, desde a operação até a estratégia.

Em uma breve análise pode-se destacar a importância da segurança da informação, especificamente para a área de TI, que com a automação dos mais variados processos empresariais tornou-se responsável por organizar, estruturar, manter, armazenar e proteger as mais diversas e variadas informações das organizações. Assim, sendo o primeiro alvo, é a porta de entrada das ameaças à informação.

INTRODUÇÃO

A disciplina de Segurança da Informação deverá demonstrar as principais técnicas para proteção dos ativos de informações nas organizações e como os profissionais de tecnologia da informação devem utilizar tais mecanismos.

A preocupação com a segurança das informações deve ser de cada um, não limitado apenas do ambiente corporativo. O cenário tecnológico atual tornou a informação mais rápida, acessível e extremamente sensível a furtos, mau uso, perdas ou falhas sistêmicas.

O desafio dos profissionais diante desse cenário é de criar mecanismos para evitar que as informações, por algum motivo, deixem as organizações vulneráveis às ameaças que são certamente reais e imediatas.

Quando o assunto é segurança da informação estamos imediatamente nos referindo a criar mecanismos para proteger as informações sobre três componentes básicos:

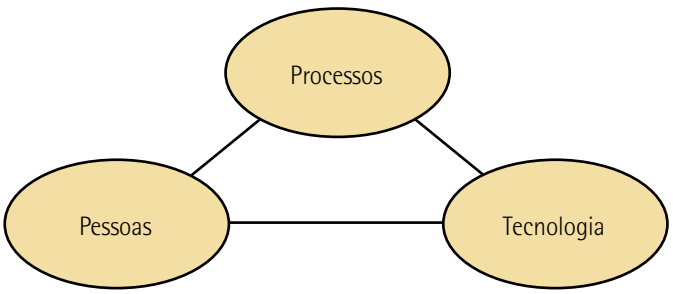

Figura 1 – Os componentes de proteção da Segurança da Informação

Toda e qualquer ameaça explorará as vulnerabilidades contidas em um desses três componentes. Quando falamos em segurança da informação, não existe a ideia de algo 100% seguro e protegido. Outra realidade é que quando falamos em processo e em tecnologia, a introdução de técnicas, tecnologias, padronizações, organização e disciplina torna possível atingir patamares eficazes de proteção, como será demonstrado no decorrer dos estudos. Porém, diante dessa situação, as pessoas representam o grande desafio para a segurança da informação, pois estão mais vulneráveis à ação das ameaças à segurança da informação.

Algumas referências bibliográficas nomeiam os componentes de segurança da informação de "corrente da segurança da informação", em que a força de uma corrente é verificada a partir de seu elo mais frágil. No caso da corrente de três elos, apresentada aqui, as pessoas são o elo mais frágil e que requer mais atenção, ou seja, de nada adianta todo o aparato tecnológico de segurança se as pessoas não estão devidamente preparadas, instruídas, conscientizadas e treinadas para tal.

Unidade I

1 PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Os conjuntos de dados agrupados formam a informação, que assim que definida pode ser utilizada nas mais diversas fontes, meios, canais e organizações.

A segurança da informação, como muitos poderiam supor, não é baseada apenas em recursos tecnológicos, apesar de extremamente necessários e amplamente utilizados. Existem ativos de informação que estão armazenadas apenas na mente das pessoas ou escritas em papel, por exemplo.

> Segurança da Informação pode ser entendida como o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade (BEAL, 2008, p. 1).

As ações voltadas para proteger os ativos de informação estão sempre baseadas nos princípios de integridade, disponibilidade e confidencialidade, ressaltando apenas que os princípios de legalidade e legitimidade podem ser adicionados, formando os pilares da segurança da informação demonstrados na figura a seguir:

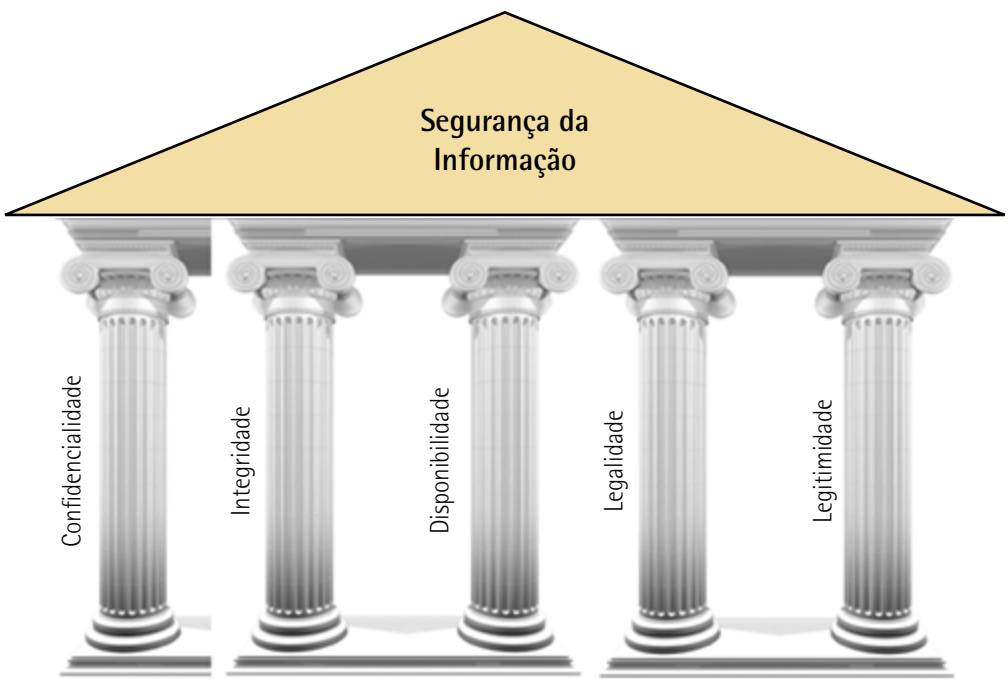

Figura 2 – Pilares da Segurança da Informação

Beal (2008) define o princípio de confidencialidade como a garantia de que o acesso à informação seja dado apenas para aqueles usuários legitimados a acessar a informação.

O principio de integridade remete à responsabilidade de garantir que as informações não sofram alterações em todos os seus estados possíveis.

De acordo com Beal (2008), disponibilidade é a garantia de que a informação esteja disponível para os usuários legitimados no momento em que estes fizerem a requisição do seu acesso.

O aspecto de legalidade remete a garantir que a informação esteja seguindo os aspectos de conformidade com as leis vigentes. Garantir a legitimidade é assegurar que as informações não sejam utilizadas por usuários não autorizados.

A transmissão da informação em um processo de comunicação requer atenção especial, pois nesse momento a informação trafegará de um ponto a outro, o que abre margem para incorrer em problemas como interceptação e alteração fraudulenta de documentos. Por esse motivo, as organizações precisam adotar processos adicionais para garantir a segurança da informação no processo de comunicação.

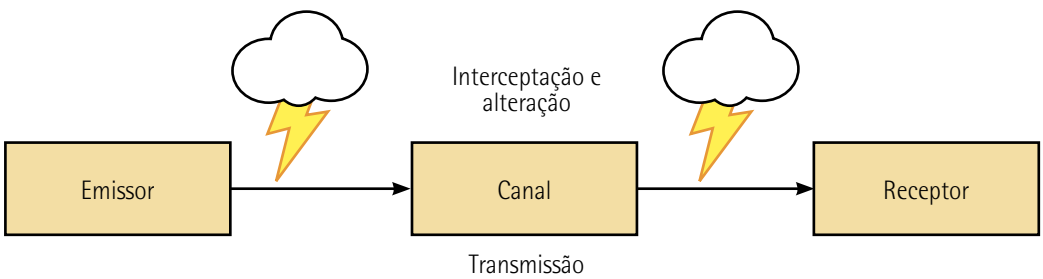

Figura 3 – Processo de comunicação adulterado

Diante desse cenário vulnerável é necessária a adoção de procedimentos de segurança para proteger as informações e assegurar a comunicação de um ponto a outro.

Segundo Beal (2008), garantir a integridade do conteúdo da mensagem é assegurar que a mesma que foi enviada pelo emissor chegue ao receptor de forma completa e exata.

A irretratabilidade da comunicação é a garantia de que a comunicação da mensagem foi realmente bem-sucedida, evitando assim que o emissor ou o receptor negue esse fato.

A autenticidade do emissor e do receptor é garantir que a pessoa emissora ou receptadora é realmente quem diz ser no processo de comunicação. Ou seja, é preciso assegurar a confidencialidade do conteúdo de modo que apenas os destinatários possam ter acesso ao conteúdo da informação.

Por fim, é preciso ter em mente que, caso ocorram problemas na comunicação, deve haver uma capacidade de recuperação do conteúdo pelo receptor em sua forma original.

Observação

Beal (2008) define o Ativo de Informação simplesmente como qualquer dado ou informação que esteja vinculado a um valor para o negócio.

1.1 Ciclo de vida da informação

Toda informação é perecível e possui prazo de validade, o que determina o seu ciclo de vida. Os diversos estágios deste ciclo de vida devem possuir formas diferenciadas para o seu tratamento, manutenção e implantação de mecanismos de proteção, motivo pelo qual é fundamental entender o que cada etapa do ciclo de vida da informação necessita.

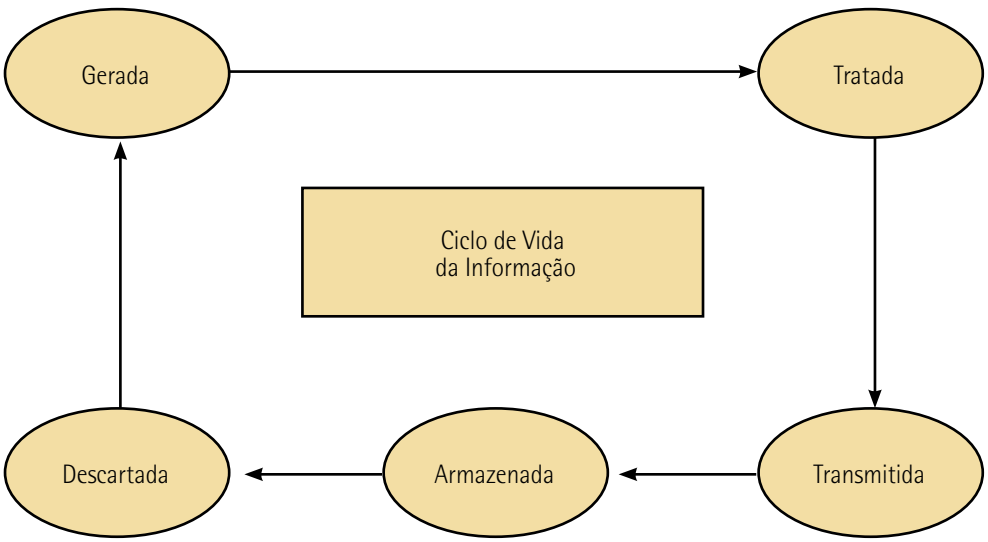

Figura 4 – Ciclo de vida da informação

A geração da informação é marcada por sua aquisição e por sua criação no ambiente interno. Além disso, ela pode ser retirada de banco de dados, de mídias, da internet e de outras fontes de informação, ou simplesmente herdada de uma área ou empresa.

Após sua geração, a informação passa pela fase de tratamento e manipulação, período pelo qual ela é estruturada, organizada, modificada, agrupada ou condensada para se transformar em um autêntico ativo de informação.

A etapa seguinte se refere à transmissão da informação que, por algum motivo, será passada de um ponto a outro por meio de algum canal de comunicação, como os canais estruturados (*e-mails*, internet, *links* dedicados) e os canais não estruturados (a voz).

Na fase de armazenamento, os ativos de informação que não estão sendo ou que já foram tratados ou transmitidos devem ser devidamente guardados de forma organizada para possíveis consultas futuras. Os locais mais comuns de armazenamento são os arquivos físicos e os bancos de dados.

A fase de descarte ocorre quando a informação, por não ser mais necessária, é finalmente excluída do rol de informações da organização. Apesar de não ter mais importância, o descarte inadequado pode ainda assim causar prejuízos à segurança da informação.

1.2 Componentes de segurança da informação

A segurança da informação deve compreender diversos cenários para, assim, estar habilitada a traçar um plano eficaz de proteção aos ativos de informação.

1.2.1 Proteções

Proteções podem ser definidas como medidas que são adotadas para proporcionar segurança aos ativos de informação. Cabe ressaltar que o balanceamento entre o custo e o benefício são fundamentalmente necessários.

As proteções são implantadas sob três aspectos:

Quadro 1 – Exemplos de medidas de proteção

Tipo de proteção	Exemplos
Lógica	Permissões em sistemas de arquivos *Firewalls* Perfis de usuários em aplicações
Física	Portas Fechaduras Vigilantes
Administrativa	Políticas Normas Procedimentos

Observação

Firewalls são dispositivos de controle de acesso em redes de dados. Veremos mais detalhamente sobre esse dispositivo no decorrer de disciplina.

A implantação de mecanismos de proteção isolados não são suficientes para evitar os ataques, razão pela qual uma forma eficaz de implementação de mecanismos se baseia na utilização de mecanismos em camadas. Nesse mecanismo, uma atua como contingência da outra, como portas a serem ultrapassadas, de modo que, caso o atacante consiga abrir uma porta, outra diferente se apresentará como proteção.

Quadro 2 – Exemplos de medidas de proteção por camadas

Nível	Tipos de Proteção	Descrição
00	Preventiva	Evita que incidentes ocorram
01	Desencorajadora	Desencoraja à prática de ações
02	Limitadora	Diminui danos causados
03	Monitoradora	Monitora estado e funcionamento
04	Detectora	Detecta a ocorrência de incidentes
05	Reativa	Reage a determinados incidentes
06	Corretiva	Repara falhas existentes
07	Recuperadora	Repara danos causados

1.2.2 Valor

É referenciado pela importância que o ativo tem para a organização. Esse valor pode ser medido de forma mensurável, como o valor financeiro e o lucro, mas também pode ser medido de forma abstrata, como o comprometimento da imagem da empresa.

1.2.3 Ameaças à segurança da informação

Evento que tem potencial para causar prejuízos aos ativos de informação da organização, trazendo dessa forma danos diretos (roubos) ou prejuízos com situações inesperadas (incêndio).

1.2.4 Vulnerabilidade

A simples ausência de mecanismos de proteção apropriados ou falhas em mecanismos de proteção existentes podem acontecer. Vulnerabilidades são a porta de entrada para que as ameaças se concretizem.

1.2.5 Impacto

Refere-se ao tamanho do prejuízo que uma determinada ameaça causará, prejuízo esse que pode ser medido a partir de propriedades mensuráveis ou abstratas.

1.2.6 Risco

Medida que indica a probabilidade de uma determinada ameaça explorar uma vulnerabilidade e assim se concretizar. O risco combinado ao impacto gera uma métrica muito explorada pela segurança da informação.

1.3 Segurança da informação baseada na Tecnologia da Informação

Tecnologia da Informação (TI): solução ou conjunto de soluções sistematizadas baseadas no uso de métodos, recursos de informática, de comunicação e de multimídia que visam a resolver problemas relativos à geração, tratamento,

> processamento, armazenamento, veiculação e reprodução de dados, e a subsidiar processos que convertem dados em informação (BEAL, 2008, p. 8).

Ainda segundo Beal (2008), grande parte das informações e dos dados importantes para as organizações é armazenada em computadores. Isso demonstra o quanto elas dependem da fidelidade da informação fornecida pelos seus sistemas baseados em TI.

Podemos compreender como informações baseadas em TI todas aquelas residentes em bases de dados, arquivos informatizados, mídias magnéticas etc., ou seja, tudo aquilo que exija soluções informatizadas para acesso.

Deve-se ter a devida preocupação em relação à segurança da informação por quatro importantes razões:

1. **As empresas estão cada vez mais dependentes da tecnologia da informação:** os sistemas devem oferecer serviços adequados e no tempo certo para a sobrevivência das organizações.

2. **Vulnerabilidades da infraestrutura:** a composição de um ambiente estável é necessário uma vez que os componentes de *hardware* e *software* poder ser alvos dos mais diversos importunos, desde a origem natural, passando por acidental, chegando ao intencional.

3. **O alto valor da informação armazenada:** as informações armazenadas em sistemas de TI requerem maior grau de proteção por serem uma atrativo para espiões e até mesmo empregados dispostos a abusar de seus privilégios em troca de dinheiro ou vantagem oferecida.

4. **A pouca atenção dada à segurança nos estágios iniciais do desenvolvimento de *software*:** preceitos de segurança da informação devem acompanhar o desenvolvimento dos sistemas desde seu planejamento primário.

Saiba mais

Para conhecer mais sobre a importância da TI para as empresas e sua relação com a segurança da informação, acesse o seguinte *site*:

<http://computerworld.uol.com.br/tecnologia/2011/07/23/seguranca-da-informacao-ha-sintonia-entre-ti-e-negocios>. Acesso em: 9 jan. 2012.

1.4 Origem dos problemas e estratégias de proteção

A origem dos problemas de segurança está baseados em três fontes diferentes: natural, acidental ou intencional, sendo que as duas últimas estão diretamente relacionadas ao fator humano.

Quadro 3 – Origem dos problemas

Origem do Evento	Exemplos
Natural	Fenômenos meteorológicos
Acidental	Erros de usuários Falhas nos sistemas Falta de energia elétrica
Intencional	Invasões Terrorismo Chantagem e extorsão Espionagem e inteligência competitiva

Diante da origem dos problemas são elaboradas as estratégias de proteção, que por sua vez podem criar mecanismos de proteção para mais de um dos problemas mensurados.

Com o passar dos anos, as estratégias de proteção estão ganhando importância em virtude do aumento potencial dos incidentes de segurança das mais diversas formas. Durante o estudo de nossa disciplina veremos variadas formas de estratégias de proteção, ressaltando que todas visam a proteger contra uma ou mais das três origens de problemas, como mencionado.

- **Estratégia de privilégio mínimo:** consiste em dar permissão mínima de acesso dos usuários aos sistemas, ou seja, fornecer apenas o acesso necessário para que usuário desenvolva suas atividades e nada mais. Assim, evita-se o excesso de acessos nos mais variados sistemas e consequentemente se reduz a possibilidade de erro nas permissões de acesso, preservando a confidencialidade das informações.

- **Estratégia de defesa em profundidade:** consiste em colocar vários mecanismos de proteção para proteger o mesmo ativo. Isso funciona semelhantemente a uma casa com diversos níveis de proteção que funcionam como barreiras inibidoras, ou seja, primeiramente o portão, depois a porta de entrada. Essa estratégia de proteção funciona como uma contingência da outra.

- **Estratégia do elo mais fraco:** a força da corrente é determinada pela força de seu elo mais fraco. Essa estratégia consiste em encontrar onde está a parte mais fraca nos processos – se é nas pessoas ou na tecnologia – e ali adicionar maior carga de mecanismos de proteção para equilibrar a corrente.

- **Estratégia do ponto de estrangulamento:** processo muito simples que funciona como a recepção de um prédio. Consiste em concentrar em um único local toda a permissão de acesso, ou seja, todos devem passar por um único controle de acesso, como uma espécie de funil, forçando assim o fluxo de proteção por um único canal, o que deixa a implantação de mecanismos de proteção mais barata e muito útil. Essa estratégia é muito utilizada para garantir a proteção em rede de dados, conforme será demonstrado no decorrer da disciplina.

- **Estratégia de segurança por meio da obscuridade:** consistindo em esconder a existência de um ativo de informação, este tipo de estratégia parte do pressuposto de que se os atacantes não sabem da existência do ativo, não haveria interesse em furtá-lo. É a forma mais simples de proteção.

Lembrete

Os profissionais de tecnologia da informação devem estar cientes de que, por vezes, a origem dos problemas de segurança da informação está atrelada ao fator humano.

1.5 Classificação da informação

A organização de qualquer item de informação deve passar primeiramente por uma análise de seu grau de importância, que é determinado sempre pelo seu proprietário. Ninguém abandonaria o seu diploma universitário em um local que certamente seria destruído, por exemplo, porém pode ser que uma ou outra pessoa não se importaria com isso.

Segundo Kovacich (1998), apesar de não existir uma forma padronizada de se classificar a informação de uma organização, podemos separá-la em três categorias:

Quadro 4 – Categoria de informações

Categoria	Tipo de informações
Informações pessoais	Dados individuais de empregados, cliente e outras pessoas.
Informações de segurança nacional	Informações que precisam ser protegidas para garantir a segurança da sociedade e do Estado.
Informações de negócio	Informações utilizadas pelas organizações para desempenhar suas tarefas.

Na prática, o processo de classificação da informação consiste em organizar as informações pelo seu grau de importância e, a partir daí, definir quais os níveis de proteção que cada ativo de informação requer. Dessa forma, evita-se a implantação desnecessária de mecanismos de proteção para ativos de pouca importância e também que sejam aplicados mecanismos inferiores para ativos sensíveis ou extremamente importantes, o que os deixaria vulneráveis.

Podemos mensurar os objetivos básicos da classificação da informação em:

- **Proteção:** as organizações manipulam diversos ativos de informação, os quais podem estar passando por qualquer fase do ciclo de vida. Por essa razão, é necessário avaliar cada ativo para saber em que fase ele está e qual o nível de proteção que será aplicado, atingindo, dessa forma, o máximo de eficácia possível no uso do mecanismo da proteção.

- **Economia:** quanto maior a necessidade de proteção para o ativo, maior será o investimento financeiro em mecanismos de proteção. Na prática isso quer dizer que, se a classificação das informações representar a realidade, isso representará economia para organização, uma vez que estará aplicando seu dinheiro em mecanismos que protegerão seus ativos mais importantes.

O processo de classificar as informações traz diversos benefícios para uma organização. Assim, dos benefícios tangíveis, podemos mencionar:

Quadro 5 – Benefícios tangíveis da classificação da informação

Benefício	Descrição
Conscientização	O envolvimento das pessoas no processo de classificação das informações pode ser um auxiliador na implantação e no processo de melhoria contínua.
Responsabilidades	Define um responsável por cada ativo de informação da organização e assim define quem deverá classificar a informação.
Níveis de proteção	Um efetivo e bem aplicado programa de classificação da informação é a maneira mais eficaz de proteger as informações que são realmente importantes.
Tomada de decisões	Uma vez que as informações estão bem categorizadas do ponto de vista da segurança, o processo de tomada de gestão da segurança da informação é facilitado.
Uso de recursos	A classificação eficaz das informações evita o desperdício de recursos de forma indiscriminada.

A classificação da informação não é imutável. Pelo contrário, assim como a informação passa por um ciclo de vida, sua classificação pode mudar conforme seu estado e importância, a exemplo do balanço patrimonial de uma empresa que inicia seu ciclo de vida classificado no nível mais alto e que termina seu ciclo de vida publicada nas mídias com o menor nível de classificação possível.

Assim, podemos dizer que não existe um modelo padrão para a classificação da informação. É recomendado que sejam definidos ao menos três níveis de classificação, mas também não muito mais que isso para não dificultar a organização. Essa definição de níveis auxilia na identificação e na implantação dos critérios e dos mecanismos de proteção.

A classificação da informação pode ter diversas formas, dependendo de qual dos princípios ela pretende atender, e sua rotulação deve seguir o ponto de vista determinado e suas exigências.

De acordo com o princípio de confidencialidade das informações, dependendo de sua importância, deve-se preservar o seu sigilo a fim de que apenas as pessoas autorizadas tenham acesso a tais informações, tanto que, para alguns casos, manter a confidencialidade é uma exigência legal.

Algumas questões devem ser respondidas para aqueles que determinam a classificação da informação sob o aspecto da confidencialidade, como: "O que aconteceria se alguém sem autorização de acesso à informação de repente obtiver tal acesso?".

Quadro 6 – Exemplo de classificação pública federal de documentos. Decreto nº 4.553/2002

Categoria	Tipo de informações
Ultra secretas	Aquelas cujo conhecimento não autorizado pode acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.
Secretas	Aquelas cujo conhecimento não autorizado pode acarretar dano grave à segurança da sociedade e do Estado.
Confidenciais	Aquelas que, no interesse do Poder Executivo e das partes, devem ser de conhecimento restrito, cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.
Reservadas	Aquelas cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

As organizações podem seguir diversos esquemas de classificação para suas informações no que se refere à confidencialidade. Muitas atribuem apenas três categorias para facilitar a análise e a implantação de mecanismos de proteção. São elas: confidencial, restrita e pública.

Para o princípio de disponibilidade, a preocupação é de como recuperar as informações e de como manter essas informações sempre disponíveis aos usuários com acesso autorizado.

Diante desse princípio, a classificação dos ativos de informação é estabelecida pelo tempo que a informação pode ficar inacessível aos usuários legitimados. Sendo assim, quanto menor esse tempo de inacessibilidade, maior será a sua categoria de classificação.

Já o princípio de integridade tem como objetivo classificar os ativos de informação a fim de que a integridade seja preservada e que, sob hipótese alguma, seja modificada ou adulterada.

Por último, temos o princípio de autenticidade, que deriva do princípio de integridade e que tem como objetivo a legitimização da informação, criada por alguém com autoridade para fazê-lo e oriunda da fonte à qual é atribuída (BEAL, 2008, p. 69).

Os exemplos mais comuns são de informações que serão destinadas ao público externo, os quais requerem por si a verificação da autenticidade.

Quadro 7 – Exemplo da classificação da informação quanto aos requisitos de autenticidade

Tipo	Características	Exemplo
Com exigência de verificação de autenticidade	Informação cuja procedência precisa ser confirmada antes de sua utilização	Pedido de criação de senha de acesso para um usuário de sistema, comunicados públicos em nome da organização, informações relativas a transações financeiras, sistemas de publicação eletrônica disponíveis para o público
Sem exigência de verificação de autenticidade	Informação cuja procedência não precisa ser confirmada antes do seu uso ou divulgação	

Fonte: BEAL, 2008, p. 69.

A classificação dos ativos físicos, de *softwares* e de serviços não é uma tarefa das mais fáceis. Por essa razão, geralmente ela pode ser feita com a criação de grupos de ativos levando em conta limites pré-estabelecidos por características comuns, como os tipos de usuários. Como resultado, essa segmentação dos ativos proporciona a oportunidade de criação de estratégias diferenciadas de proteção.

Quadro 8 – Exemplo da classificação da informação por segmentos

Segmento	Ativos físicos, *software* e serviços
Por pessoas	A segregação dos horários de trabalho por cargos
Por processos	O agrupamento de aplicações e equipamentos por tipo de processos associados, classificados por sua relevância ao negócio
Por tecnologia	Controle rígido de acesso aos sistemas por meio de mecanismos de autenticação diferenciados para sistemas que necessitam de maior segurança

> É impossível estabelecer um modelo único de segmentação de ativos físicos, de *software* e de serviços capaz de atender às necessidades de todos os tipos de organização. Os esforços gastos no desenvolvimento de uma forma de classificação e segmentação desses ativos adaptada às características e necessidades próprias do negócio, são recompensados pelo entendimento claro dos diferentes requisitos associados aos diferentes objetivos de segurança (BEAL, 2008, p. 70).

A responsabilidade pela classificação dos ativos de informação recai sobre alguns fatores que são fundamentais neste processo de classificação nas organizações.

O fato de classificar a informação recai em sujeitá-las a determinados mecanismos de proteção e assim investir financeiramente na proteção desses ativos. Algumas organizações preferem criar um nível básico de proteção para todas as informações classificadas e nenhum nível de proteção para as não classificadas.

Podemos dizer que a informação tem vida, motivo pelo qual por vezes é necessária sua reclassificação. Assim, é importante que as organizações tenham processos formalizados e padronizados de reclassificação dos ativos de informação.

A desclassificação das informações acontece no ciclo final de vida (em seu descarte), quando, por fim, a informação será devidamente apagada por não mais ser útil à organização.

As atribuições dos processos de classificação, reclassificação, desclassificação, introdução e manutenção dos mecanismos de proteção para os ativos de informação que deveriam ser elaborados e mantidos exclusivamente pelo proprietário da informação, geralmente acabam por recair sobre os gerentes de área.

Logo abaixo do proprietário da informação vem o chamado custodiante da informação, que é aquele que de alguma forma zela pelo armazenamento e pela prevenção de informações que não lhe pertencem, mas que dela faz uso em suas atividades cotidianas.

Existem dois tipos de custodiantes:

1. Os profissionais de perfil técnico responsável pela administração e pelo funcionamento de algum sistema.
2. O proprietário de processo, que é a pessoa responsável por um processo de negócio que utiliza informações que não lhe pertencem, mas que fazem parte do processo sob sua responsabilidade.

A equipe de segurança é responsável por ser o ponto de apoio das áreas de negócio, de forma a desenvolver, implementar e monitorar estratégias de segurança que atentem aos objetivos propostos de proteção dos ativos de informação.

Já os gerentes de usuários têm a responsabilidade de responder sobre a ação dos membros de sua equipe e também de multiplicar o conceito de classificação determinado pela organização.

Por sua vez, os usuários finais dos ativos de informação são os principais responsáveis pela execução das recomendações de classificação da informação, uma vez que estão diretamente ligados ao operacional.

Observação

A tarefa de classificação da informação é dada aos mecanismos de proteção, porém ela por si própria não consegue proteger as informações, pois como é possível aplicar os mecanismos apropriados se o que é importante proteger ainda é desconhecido? Essa é a tarefa da classificação da informação.

A implantação de mecanismos de controle após o processo de classificação da informação visa a assegurar a proteção dos seus ativos. Os mecanismos mais comuns são aqueles que têm o objetivo de proteger a confidencialidade das informações das organizações, no entanto, a integridade e a disponibilidade também devem ser protegidas. Assim, podemos dividir os mecanismos de proteção sob as esferas da proteção dos dados, proteção física e controles administrativos:

Quadro 9 – Exemplo de mecanismos de proteção ligados à classificação da informação

Esferas	Exemplos de mecanismos aplicados
De dados	Criptografia *Backups* Sistemas redundantes Controle de acesso
Física	Controle de acesso físico Cofres Circuito fechado de TV Transporte seguro
Administrativa	Políticas Revisão e aprovação Separação de tarefas Monitoramento

A proteção na esfera de dados se destaca pelo uso da criptografia, que é uma das principais tecnologias existentes para proteger as informações. Por meio desse mecanismo é possível disponibilizar uma série de serviços de forma segura e eficaz, mantendo a confidencialidade, a disponibilidade e a integridade das informações.

Observação

Detalhes sobre o que é, os tipos e onde se aplica um processo criptográfico serão dispostos no decorrer da disciplina.

O uso de cópias de segurança, também conhecidas como *backups*, tem a finalidade de armazenar as informações de um sistema, criando um mecanismo de recuperação dos arquivos em caso de falha na informação original.

Os sistemas redundantes, apesar de semelhantes aos backups, são utilizados em situações nas quais as informações processadas são ainda mais críticas, de modo que a organização não pode dispor delas mesmo que por um período curto de tempo. Seria como deixar um sistema secundário e semelhante parado, esperando que o sistema principal por algum motivo venha a parar de funcionar, para assim assumir seu lugar, sem interrupções.

A implantação de controle de acesso tem como missão proteger os dados contra problemas de segurança relacionados à quebra, principalmente, de confidencialidade e integridade. Sua função é garantir que apenas usuários e processos autorizados tenham acesso a determinadas informações e que possam executar apenas as ações previamente definidas.

Na esfera física obviamente temos o controle de acesso físico, no qual podemos destacar o uso de catracas e portas de acesso inteligentes, ou seja, dispositivos que impedem a entrada física de pessoas em ambientes nos quais o acesso é restrito a pessoas autorizadas.

O uso de cofres tem duas finalidades: a proteção dos ativos de informação físicos, como contratos e fitas de *backup* contra furtos e roubos, e a proteção em caso de incêndios para alguns tipos especiais de cofres.

Já para caso de furto de informações, os circuitos fechados de TV funcionam no monitoramento de áreas para resolução de incidentes, além de possuir um caráter desencorajador.

Ao ser transportada fisicamente, a informação corre uma série de ameaças. Assim, para reduzir as tais vulnerabilidades, são utilizados diversos tipos de proteções, que vão desde um envelope com um lacre inviolável até o uso de um carro forte.

Na esfera dos controles administrativos, vemos as medidas relacionadas à forma como os procedimentos devem ser executados e as necessidades de interação entre as pessoas com diversas responsabilidades. Como destaque, temos as políticas, que são o principal controle administrativo

relacionado à segurança da informação e que, consequentemente, por meio da política de classificação da informação, definem padrões de conduta, os quais são os passos necessários para a execução segura dos procedimentos.

O processo de revisão e aprovação tem como objetivo estabelecer que qualquer ação individual que tenha maior importância do ponto de vista da segurança deva ser realizada em mais de um passo, ressaltando assim a responsabilidade da execução e revisão distintas, incluindo a autorização para concretização.

Diante do processo de separação de tarefas, podemos destacar que, nesse modelo, em função da importância dos ativos de informação, é exigida a divisão de responsabilidades, pois dessa forma as pessoas que executam uma atividade não podem ser as mesmas que a aprovam, coibindo assim a ação ou a tentativa de fraude.

Para auxiliar no processo de classificação das informações, que na prática está ligada ao dia a dia das operações, temos alguns mecanismos úteis:

Quadro 10 – Aspectos práticos da classificação da informação

Práticas	Meio	Canais
Rotulação	Documentos impressos	Papéis
	Documentos eletrônicos	Arquivos eletrônicos
Controle de acesso	Físico	Tecnologias biométricas
	Lógico	*Login* de acesso a sistemas

Quando o assunto é rotulação de documentos visando à classificação da informação, a primeira coisa que surge em nossa mente são os documentos impressos. De fato, os documentos impressos são mais fáceis de rotular. A rotulação visa inibir a ação de algum fraudador, mas principalmente salvaguardar a organização no caso de violação da segurança da informação naquele nível de classificação.

Para rotular papéis, o uso de etiquetas, carimbos e outras marcas visuais são recomendados. Pode também ser inclusa no rodapé dos documentos ou até mesmo como marca d'água.

A rotulação de documentos eletrônicos requer maior atenção, pois a marca da classificação deverá ser mostrada dentro do conteúdo do documento, como na classificação no corpo da mensagem ou no campo de assunto de um *e-mail*.

Sistemas e aplicativos devem mostrar o nível da classificação de um registro visualmente ao ser acessado.

As mídias podem ser rotuladas visualmente com etiquetas, assim como os documentos impressos.

A segunda forma de criar mecanismos cotidianos é o controle de acesso, o que pode ser realizado por meio dos níveis de classificação. Essa forma de controle é o principal benefício buscado pela classificação da informação.

O controle de acesso lógico nos remete ao controle de acesso a redes e a dados. Um exemplo claro de controle de acesso lógico é durante o *login* de rede, para o qual temos de possuir um usuário válido e uma senha pessoal e intransferível de acesso para aquele segmento de rede, bem como o controle de acesso às pastas e aos diretórios dentro dos servidores.

O controle de acesso físico está ligado ao uso de ferramentas criptográficas, como os certificados digitais, que cada vez mais tem ganhado espaço entre as tecnologias para controle de acesso. O uso de biometria também tem se mostrado bastante útil nesse meio.

1.6 Estrutura da segurança da informação

Apesar de a segurança da informação não ser composta apenas por TI, esta foi a primeira área que percebeu a necessidade de proteger seus ativos. Por esse motivo, a segurança da informação nasceu atrelada às áreas técnicas das organizações, pelas quais também é subsidiada.

Para melhor compreensão da atual necessidade de segurança é preciso primeiramente compreender como se deu a evolução da área de TI durante os anos, fator esse que levou à maior exposição dos ativos de informação.

A área de TI teve seu início baseada em arquitetura centralizada, que utilizava *mainframes*. O acesso se dava por meio de terminais seriais, com a presença de todos os equipamentos concentrados em um CPD e de técnicos com alto conhecimento sobre o ambiente em questão.

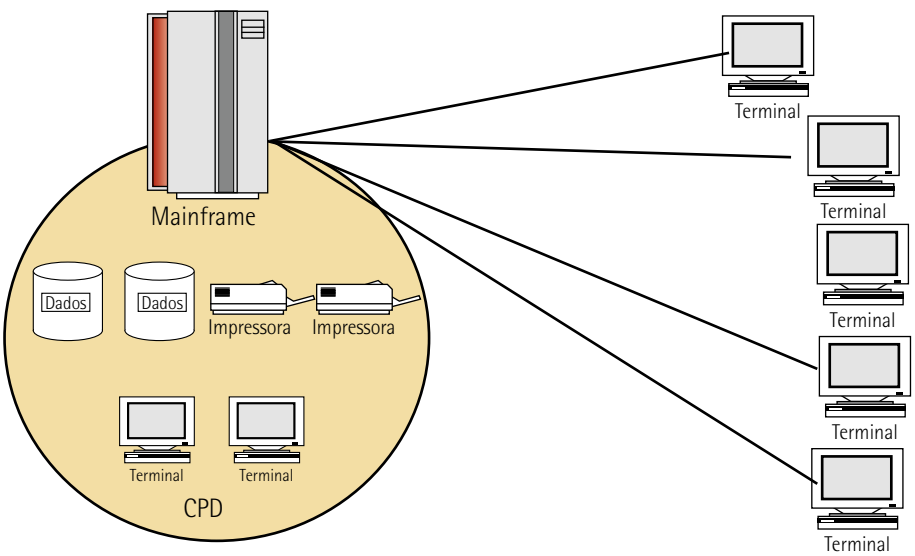

Figura 5 – Estrutura de TI do início da era computacional

Nos últimos anos a área de TI vem sofrendo significativas alterações. Os modelos atuais pulverizam as informações de tal forma que auxilia o negócio, porém a preocupação em protegê-las foram redobradas. Tais mudanças são visíveis com a descentralização do processamento computacional, o *downsizing*, a disseminação das redes locais (LAN), a disseminação das redes corporativas (MAN e WAN), a grande variedade de arquiteturas de servidores e sistemas operacionais (OS/390, Win2K, Solaris, HP-UX, Linux) etc.

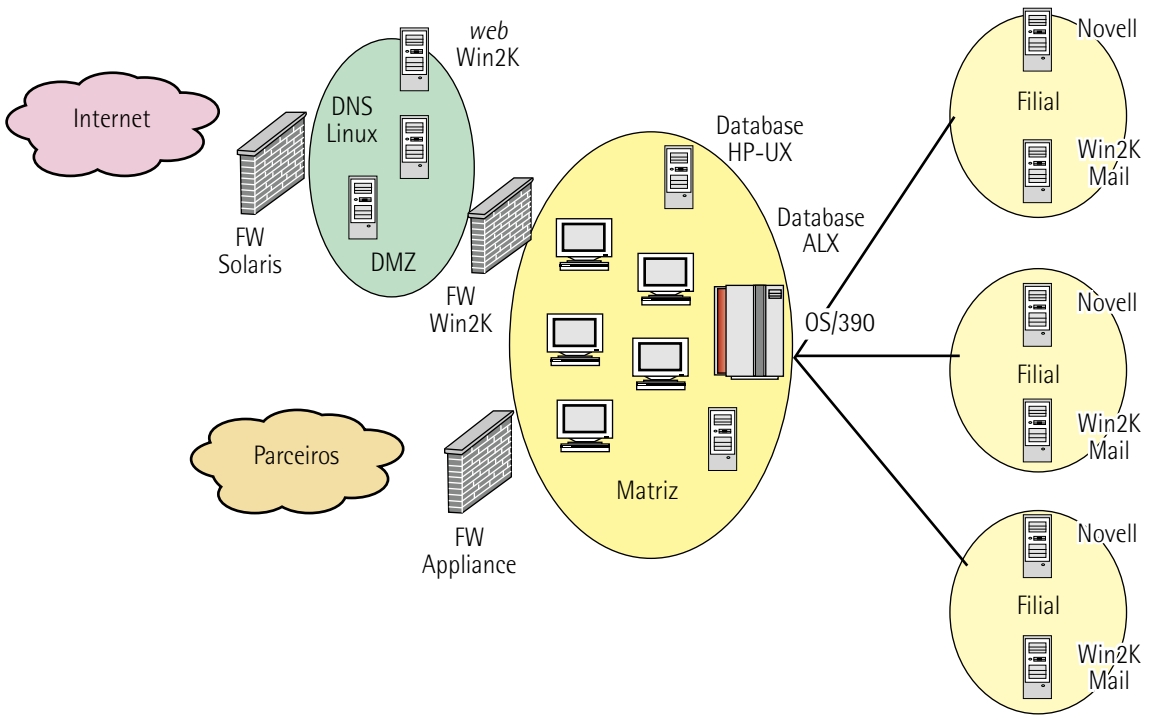

Figura 6 – Estrutura atual da TI

As consequências da nova estrutura podem ser representadas por diferentes equipes (desenvolvimento e manutenção), especializadas em determinadas tecnologias, como: equipes de alta plataforma (*Mainframe*), de plataforma Windows, de plataforma Unix, de rede local e de rede WAN.

A área de TI está sendo afetada por diversos fatores, como a evolução da forma de conduzir os negócios em razão da importância da informação, a mão de obra, a regulamentação, a governança corporativa, a dificuldade no desenvolvimento de projetos que integram plataformas diferentes, a dificuldade em manter os servidores atualizados e a dificuldade em mapear e gerenciar os riscos de TI.

Como exemplos de empresas brasileiras que têm sido cada vez mais afetadas pelas regulamentações locais e internacionais são as definidas pelo Banco Central do Brasil, como CVM, Sarbanes-Oxley, entre outras. Tais regulamentações acabam por requerer direta ou indiretamente que as empresas sigam os princípios de segurança da informação.

Observação

A lei Sarbanes Oxley (SOX), aprovada no congresso americano em 2002, teve origem nos problemas com os lançamentos financeiros das empresas norte-americanas, quando 100 das 500 maiores empresas apontadas pela revista Forbes apresentaram fraudes em seus balanços financeiros.

Para evitar situações como esta, exigiu-se que todas as empresas de capital aberto que operam na bolsa de valores norte-americana sigam integralmente os controles internos estipulados pela lei.

A estruturação da área de segurança da informação tem como objetivo lidar com a segurança dentro do ambiente de TI para, dessa forma, possibilitar maior agilidade na tomada de decisões e ações quando da verificação de incidentes que possam impactar na segurança das informações ou na imagem da empresa.

A segurança da informação dentro do organograma de uma empresa tradicional, por ter surgido a partir do impulso oferecido pela TI, ainda fica hierarquicamente abaixo de outros processos, mesmo tendo como sob sua responsabilidade os processos e as pessoas.

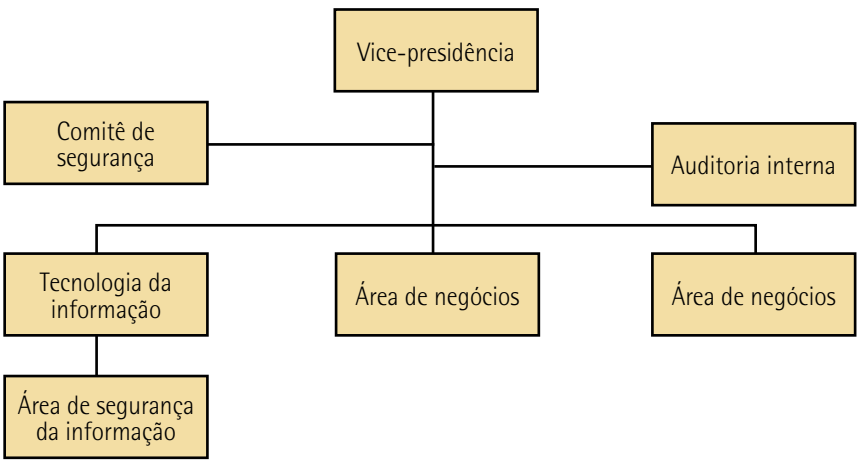

Figura 7 – Organograma tradicional

As empresas devem estar atentas para as implicações do modelo tradicional de hierarquia que coloca a segurança abaixo da TI. Com a área de segurança da informação sob gerência da TI, a tendência é que apenas os aspectos tecnológicos da segurança da informação recebam investimento, que porém por vezes não demonstram o custo/benefício das medidas adotadas.

Para que situações como essa não sejam vistas, é recomendada a alocação da área de segurança da informação no organograma da organização da seguinte forma:

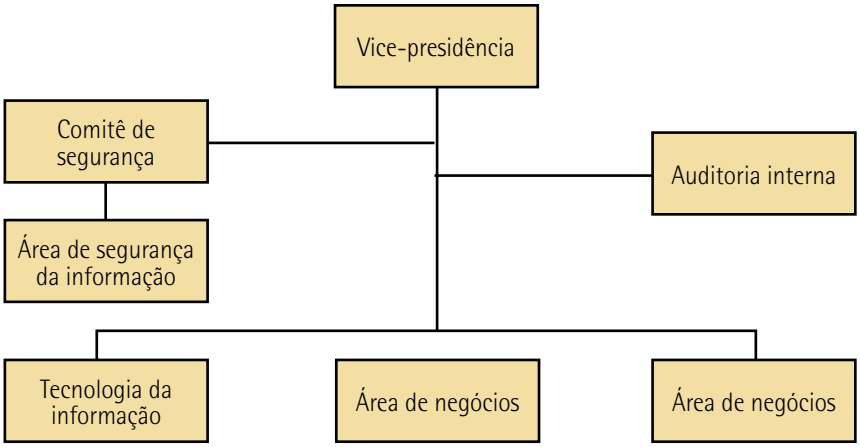

Figura 8 – Organograma ideal

Esse novo organograma proposto abre espaço para uma visão melhor da gestão da segurança da informação, pois dá a ela liberdade de atuação nos três princípios e facilita o acesso dos profissionais de segurança da informação à administração da organização para, assim, poderem exercer melhor suas diversas responsabilidades.

Dentre as atribuições estipuladas para o responsável pela área de segurança da informação (do inglês *Security Officer*), destacam-se:

- Gerenciamento das contas de acesso;
- Gerenciamento contínuo da segurança;
- Time de respostas a incidentes;
- Definição dos processos de revisão preventiva da segurança;
- Gerenciamento de novos projetos e/ou tecnologias;
- Adequação de documentos às novas tecnologias, a exemplo de: ADSL, *Wireless* (LAN e celular), VPN, *tokens* de memória, portas USB;
- Estabelecimento claro do posicionamento da empresa quanto ao uso de *e-mails*, internet, *notebooks*, *tablets*;
- Gerenciamento, desenvolvimento e implementação de políticas globais de segurança onde deve haver segmentação em políticas, normas e procedimentos, além de promover a atualização periódica destes documentos;

Lembrete

A gestão eficaz da segurança da informação em uma organização depende diretamente da liberdade de decisão que ela terá dentro de sua estrutura hierárquica.

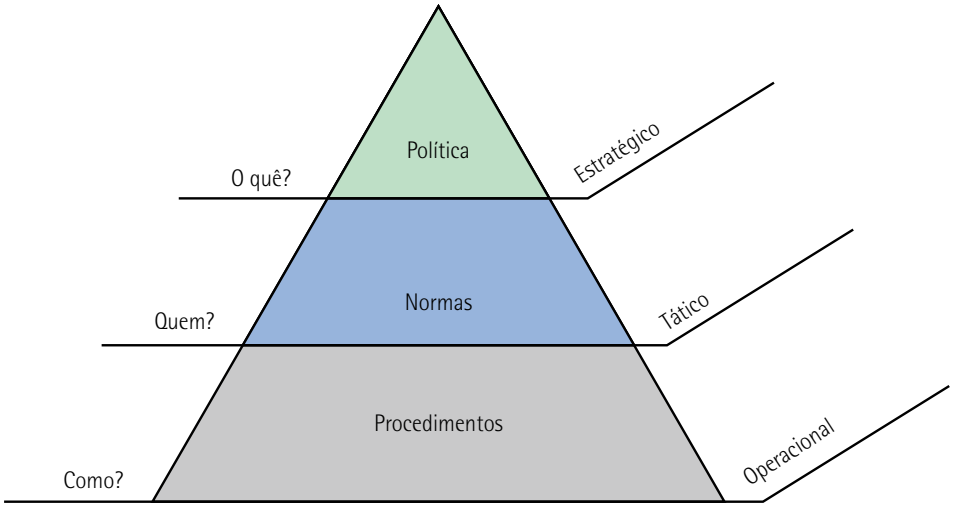

Figura 9 – Gerenciamento de normativos

- Coordenar a atividade de classificação das informações junto às diversas áreas da empresa, estabelecendo nível de confidencialidade da informação e auxiliando os gestores a classificar suas informações;
- Estabelecer controles associados ao armazenamento e à transmissão da informação;
- Disseminar a cultura de segurança, seus conceitos e práticas, tanto tecnológicas como comportamentais, junto aos colaboradores, estagiários e empresas terceirizadas;
- Responsabilidade diante das atividades de treinamento para pessoal especializado, técnico de operação (telecom, servidores, desenvolvedores), pessoal gerencial e de negócios, com palestras de conscientização destinados aos funcionários em geral;
- Gerenciamento dos perfis de todas as contas de acesso a *softwares* corporativos da organização. Devem existir informações suficientes para facilitar e agilizar a obtenção de tais dados, pois este controle é importante para assegurar que no desligamento ou em uma transferência de função o usuário não armazene acessos indevidos. Este profissional será responsável por receber, analisar, autorizar ou negar acessos aos sistemas corporativos da organização, e também por formalizar os grupos/estruturas de usuários;
- Gerenciamento contínuo da segurança, preocupação com a segmentação da rede e amplo conhecimento da topologia da rede, sendo capaz de identificar os segmentos críticos para o negócio da empresa;
- Preparo do plano diretor para mitigar as vulnerabilidades da rede e garantir a continuidade dos negócios em casos de falhas de equipamentos ou aplicações;
- Conhecer a política implementada nos *firewalls* e atuar como responsável pela autorização de concessão de acesso à rede corporativa por meio dos *firewalls*. Apesar de não ser o responsável pela configuração dessa barreira, deverá verificar continuamente o acompanhamento da monitoração dos *logs*;

- Determinar qual a política a ser implementada no IDS e qual ação deverá ser tomada em caso de identificação de ataque, além de acompanhar o processo de monitoração contínua dos relatórios gerados pelo IDS;
- Responsável pelo projeto e pelo acompanhamento da implementação do sistema de antivírus e também pela definição de normas e procedimentos relativos à atualização da base de assinaturas nas estações e nos servidores da empresa;
- Coordenar a elaboração de metodologias de instalação e manutenção segura de servidores críticos (*Bastion Host*);
- Coordenar a elaboração de procedimento formal de gerenciamento de mudanças nos ambientes críticos (*Change Management*), incluindo os ambientes de teste, homologação e produção;
- A avaliação física regular dos ambientes críticos é fundamental para assegurar a segurança física das informações;
- Elaboração e atualização do plano de continuidade de negócios, no qual devem estar previstos o teste periódico de *backups*, de *links backups* e de ativação de *site*/aplicações *backups*;
- A integração com as áreas de negócios e com a fábrica de *software* durante a especificação de novos projetos e tecnologias no que se refere à segurança dos dados;
- Definição dos processos de revisão preventiva da segurança da informação para teste de invasão, teste de invasão externa simulando a ação de um *hacker*, teste de invasão externa por um *hacker* com nível de acesso de seus parceiros de negócios ou clientes Interno, teste de invasão interna, revisão de *firewall* e revisão interna dos mecanismos de proteção de perímetro (*firewall*, IDS etc).

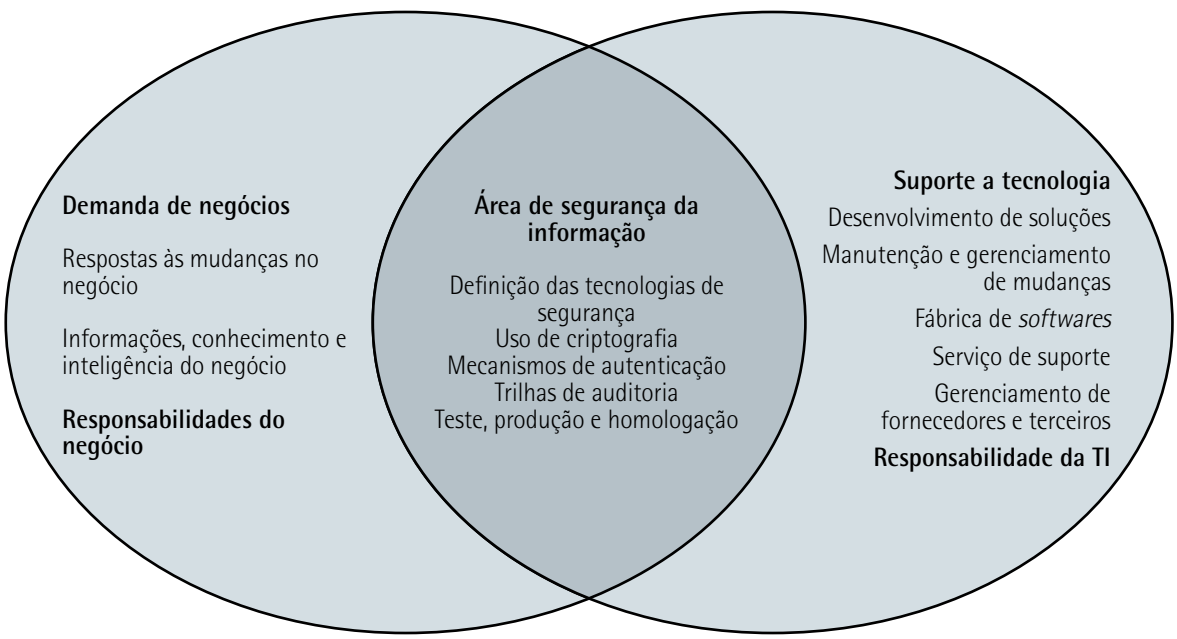

Figura 10 – Relacionamento das áreas de negócio, TI e Segurança da Informação

As pessoas selecionadas para atuar na área de segurança da informação devem possuir as seguintes habilidades:

- Ser um funcionário da corporação com ampla experiência em segurança da informação e em gerenciamento de projetos de tecnologia;
- Ser capaz de balancear as restrições de segurança com as necessidades de negócio;
- Possuir destacadas habilidades de comunicação pessoal e escrita, além de ampla capacidade de trabalho em grupo e gerenciamento de pessoas.

Nessa área, o líder – que poderá ser um gerente ou um diretor – deve saber lidar com a tomada de decisões, a requisição de auxílio de funcionários de outras áreas e a condução de verificações nas diversas áreas da corporação.

Em congruência com outras áreas, principalmente com a de tecnologia, as áreas de TI e de Segurança da Informação devem estar representadas no conselho ou na mais alta instituição da organização. Ambas precisam ser mensuradas, assim como os negócios, por meio da definição ou da reformulação do posicionamento hierárquico (CIO, CSO, CRO), e é preciso ter em mente que negócio e segurança não são elementos distintos. Entendimento dos negócios não é desenvolvimento de *software*.

O líder da área de segurança da informação não deve atuar nem como um paranóico que sempre inviabiliza o negócio nem como um cowboy que assume o risco sozinho. Cabe a ele mostrar os riscos inerentes e negociar soluções alternativas com os gestores das áreas de negócio.

2 RISCO: O QUE É, COMO AVALIAR E COMO GERENCIAR

> Tendo em vista a complexidade e o alto custo de manter os ativos de informação a salvo de ameaças à confidencialidade, integridade e disponibilidade, é de extrema importância para o alcance dos objetivos de segurança adotar um enfoque de gestão baseado nos riscos específicos dos negócios (BEAL, 2008, p. 11).

O fato de não existir nada totalmente seguro em segurança da informação obriga os gestores a conhecer ainda mais o cenário ao qual estão vulneráveis. Dessa forma, gerir os riscos nada mais é do que identificá-los e tratá-los de forma sistemática e contínua.

O processo de gestão de risco é responsável por identificar, avaliar e implementar medidas de proteções necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informações. O risco pode ser definido pela combinação da probabilidade de um evento e sua consequência.

A melhor compreensão do processo de análise de riscos passa pelo estabelecimento dos termos mais comuns utilizados para o tratamento dos riscos identificados no processo de gestão.

Quadro 11 – Termos básicos relacionados à gestão de riscos

Termos básicos	Definição
Consequência	Resultado de um evento
Critérios de riscos	Termos de referência pelos quais a relevância do risco é avaliada
Evento	Ocorrência de um conjunto particular de circunstâncias que caracterizam uma única ocorrência ou uma delas
Fonte	Item ou atividade associada a uma consequência potencial
Gestão de Risco	Coordena atividades para direcionar e controlar uma organização com relação ao risco
Probabilidade	Associada a um evento é calculada para determinar período de tempo, e é definida como número real na escala de 0 a 1

O risco é um elemento presente em todas as áreas da gestão e tem formas e formatos diferentes para cada segmento. Para a segurança da informação, o risco diz respeito a todo e qualquer tipo de situação (ou evento) que constitui oportunidade de favorecer ou prejudicar o sucesso de um empreendimento.

A ameaça é uma expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ativo de informação. Um exemplo de ameaça pode ser algo externo ao ativo, como falha de energia elétrica, fogo, vírus etc.

Beal (2008) expõe que a vulnerabilidade se resume em uma fragilidade que poderá ser explorada por uma ameaça para concretizar um ataque. A vulnerabilidade está associada ao próprio ativo, podendo ser decorrente de uma série de fatores, como falta de treinamento, ausência de manutenção ou problemas nos controles de acesso. E esse impacto é o efeito ou a consequência de um ataque ou incidente para a organização.

Esses conceitos são complementados com outros quatro conceitos que formam a gestão de riscos à segurança da informação:

- **Agente:** fonte que produz um evento que pode ter efeitos adversos sobre um ativo de informação. Exemplo: funcionários, meio ambiente e *crackers*;
- **Alvo:** ativo de informação que pode ser objeto de um ataque/incidente. Exemplo: base de dados, equipamentos de *hardware*, sistemas de informação, serviços de informação (BEAL, 2008, p. 14);
- **Ataque:** evento decorrente da exploração de uma vulnerabilidade por uma ameaça. Exemplo: vazamento de água, inclusão indevida no sistema;
- **Incidente:** evento com consequências negativas resultante de um ataque que obteve êxito.

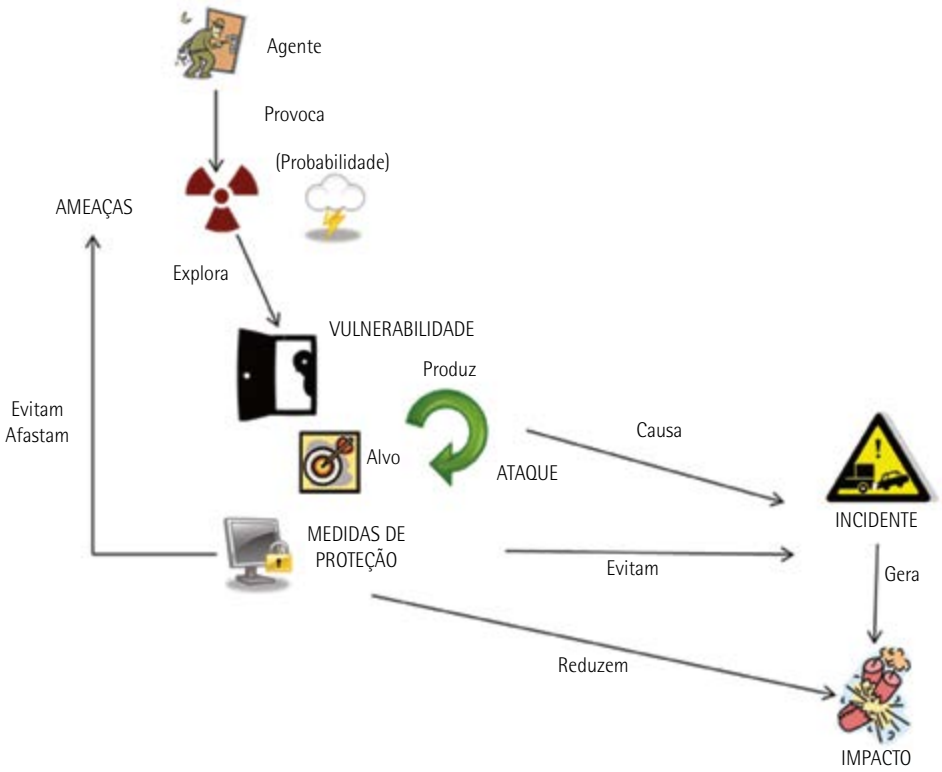

Figura 11 – Relacionamento entre os termos associados ao risco para a segurança da informação

Da acordo com Beal (2008), as ameaças são provenientes de diversas fontes e podem se aproveitar de vulnerabilidades para concretizar um ataque, o que pode vir a causar danos aos pilares da segurança da informação.

Na visão da tecnologia da informação (TI), as ameaças podem explorar uma ou mais vulnerabilidades dentro dos princípios de confidencialidade, integridade ou disponibilidade da informação.

O quadro a seguir demonstra algumas das ameaças às quais o ambiente de tecnologia das organizações está exposto e os locais afetados nos pilares da segurança da informação após o impacto.

Quadro 12 – Lista de ameaças e impactos relacionados a instalações e componentes de TI

Ameaça	Tipo de recurso vulnerável (alvo)	Impacto para o objetivo de confidencialidade	Impacto para o objetivo de integridade	Impacto para o objetivo de disponibilidade
Desastres naturais	Edifícios, torres de comunicação	Controles físicos de acesso podem ser desconsiderados no momento de pânico e informações confidenciais podem ser furtadas		Todos os serviços podem ser prejudicados e podem ficar indisponíveis
Falhas ambientais, incluindo queda de energia elétrica	*Hardware*			Serviços podem ser interrompidos e *hardwares* podem ser danificados

Furto	Equipamentos valiosos e portáteis	Equipamentos furtados podem ter informações confidenciais		Serviços podem ser interrompidos e dados podem ser perdidos
Vírus	Principalmente computadores conectados em rede		Dados podem ser corrompidos	Um vírus na rede pode interromper os serviços de rede
Falhas de *hardware*	Todo tipo de *hardware*	*Hardware* danificado pode ser enviado para manutenção contendo informações sigilosas	Dados podem ser corrompidos quando o *hardware* falhar	Serviço indisponível
Falhas de *software*	Todo tipo de *software*	Falhas nos controladores de acesso lógico podem levar à divulgação indevida de informações	Dados podem ser corrompidos	Serviço indisponível
Falha humana	Todos os sistemas	Funcionários podem divulgar informações acidentalmente ou intencionalmente	Funcionários podem inserir dados incorretos	Funcionários podem destruir informações acidentalmente ou intencionalmente

Fonte: Adaptado de Beal, 2008, p. 20.

2.1 Tratamento dos riscos à segurança da informação

O risco é a probabilidade de uma ameaça explorar uma ou várias vulnerabilidades causando danos. Geralmente está relacionado a algo negativo, porém também pode ser algo positivo. Mas, para a segurança da informação, o que é analisado e gerido é o risco no seu lado negativo da concepção.

Quando analisado pela escala negativa, o risco é determinado por dois fatores: primeiramente temos a probabilidade da ocorrência de uma ameaça, que é medida pela combinação de sua frequência com a avaliação de vulnerabilidades existentes no ambiente analisado; em segundo, temos as consequências trazidas pela ocorrência do incidente, que em segurança é chamado de impacto.

A efetiva gestão dos riscos e sua estratégia de tratamento não conseguem eliminar definitivamente o risco, motivo pelo qual a medida restante após o seu tratamento leva o nome de risco residual. O grande desafio dessa gestão é trazer o risco residual aos níveis toleráveis pelos critérios adotados pela organização, critérios esses que dependem de quanto risco ela está disposta a aceitar e como ela o percebe.

A gestão de riscos à segurança da informação está ligada a quatro atividades que determinam a forma como iremos lidar com este assunto dentro das organizações.

A primeira atividade está ligada a análise e avaliação de riscos, que por sua vez está dividida em duas etapas. Veja no quadro:

Quadro 13 – Análise e avaliação de riscos à segurança da informação

Quadro 13 – Análise e avaliação de riscos à segurança da informação

Análise e avaliação de riscos		
Análise de riscos	Identificação das ameaças	Identificar as ameaças a partir de base de dados, listas de discussão etc.
	Estimativa do risco	Atribui valores aos componentes de risco. Impactos e probabilidades, ameaças X vulnerabilidades
Avaliação de riscos	Comparação dos riscos	Decidir a forma de tratamento ou aceitação do risco

A melhor forma de analisar e avaliar o risco está no uso de uma metodologia, que pode ser classificada como quantitativa ou qualitativa.

Beal (2008) demonstra que os métodos quantitativos de avaliação de risco são úteis quando se tenta buscar um equilíbrio entre o custo de implementação das medidas de segurança e o possível custo da não implementação desses mecanismos. A forma mais conhecida dessa metodologia é o método de cálculo da expectativa de perda anual ALE (do inglês *Annual Loss Expectation*).

Para entendermos o cálculo da ALE é necessário compreender alguns conceitos, como o fator de exposição EF (do inglês *Exposure Factor*), que representa o quanto o valor do ativo será afetado pela concretização da ameaça. É importante ressaltar que o cálculo da EF apenas é utilizado para os casos em que o prejuízo foi gerado no próprio ativo.

O EF (fator de exposição) é utilizado para compor o cálculo da expectativa única de perda o SLE (do inglês *Single Loss Expectancy*), o qual representa o prejuízo causado por uma ocorrência da ameaça. Apenas para reforçar, o seu cálculo pode ou não utilizar o EF, uma vez que este é utilizado somente quando existe o prejuízo no próprio ativo.

Dessa forma, o cálculo do SLE pode ser definido de duas formas:

SLE = Valor do Ativo X EF

ou

SLE = Prejuízo causado pela ameaça

Para que seja possível calcular a ALE é necessário avaliar o risco por um período maior de tempo, estimando o número de ocorrências da ameaça em questão que esperamos sofrer ao longo deste período.

O período utilizado geralmente é de um ano, número esse representado pelo índice anualizado de ocorrência, o ARO (do inglês *Annualized Rate Occurrence*. Se esperarmos que a ameaça ocorra dez vezes por ano, então o ARO é igual a dez.

Após o cálculo do ARO fica fácil calcular o ALE:

$$ALE = SLE \times ARO$$

Por meio desse método é possível tomar decisões em relação a investimentos em segurança (BEAL, 2008, p. 22).

Como benefício da metodologia quantitativa está o rigor matemático, o que atribui mais confiança ao processo e aos resultados, além de permitir uma possível auditoria independente dos dados que foram utilizados para os componentes de risco. A referenciação financeira dos dados sobre os riscos alinha a segurança da informação com a administração da organização.

Apesar de o trabalho envolver para sua elaboração uma imensa gama de tempo de recursos, o que muitas vezes pode tornar o trabalho de análise impraticável, outra limitação desta metodologia reside no fato de não existir uma norma específica para esse tipo de análise, também inibindo a sua implantação.

Já no método qualitativo, são estimados os componentes do risco que são trabalhadas com menções mais subjetivas, como alto, médio e baixo. Dessa maneira não são mensurados valores numéricos para os componentes de risco, o que torna o processo mais rápido. Em contrapartida, esse processo obriga que os responsáveis pela análise possuam conhecimentos mais avançados sobre os componentes de risco e sobre a organização.

Quadro 14 – Exemplo de matriz qualitativa de risco

Risco baixo	De 1 a 6
Risco médio	De 7 a 12
Risco alto	De 13 a 27

Níveis	Alto	Médio	Baixo
Valores	3	2	1
Risco = Vulnerabilidade X Ameaça X Impacto			

Ameaça		Alta			Média			Baixa		
Vulnerabilidade		A	M	B	A	M	B	A	M	B
Impacto ou valor do ativo	A	1	2	3	2	4	6	3	6	9
	M	2	4	6	4	8	12	6	12	18
	B	3	6	9	6	12	18	9	18	27

No exemplo, são dispostos os dois componentes de risco – o impacto e a probabilidade –, sendo avaliados por meio de formas subjetivas. No caso da probabilidade, temos ainda seus dois componentes – ameaça e vulnerabilidades –, que também são avaliadas da mesma forma.

Na tabela, esta entrecruzada dos julgamentos leva a uma escala numérica que, por sua vez, é avaliada perante uma segunda tabela que define o que é risco alto, médio e baixo. Nessa matriz estão dispostos três níveis de avaliação, mas como esse não é o padrão, recomenda-se que sejam dispostos no mínimo três e no máximo cinco, pois mais do que isso torna o processo desnecessariamente complicado, como já foi dito anteriormente.

Os benefícios da metodologia qualitativa residem na velocidade e na menor demanda de recursos. Em última análise estão os benefícios para a gestão, que facilmente podem identificar, de forma visual, os riscos que precisam ser priorizados.

Como limitadores para a metodologia qualitativa, a falta de dados mais concretos que possam ser utilizados como subsídio para a avaliação da eficácia financeira dos investimentos cria um ponto de atenção para a gestão de risco.

Se comparadas as duas metodologias, ambas demonstram suas vantagens e desvantagens, porém o método qualitativo é o mais utilizado em razão de sua agilidade e facilidade de entendimento e implantação.

A segunda atividade refere-se ao tratamento do risco identificado nessa atividade. Para reduzir os riscos, são selecionados e implementados mecanismos que visam trazer os riscos a níveis aceitos pela organização e definidos pelos critérios de risco.

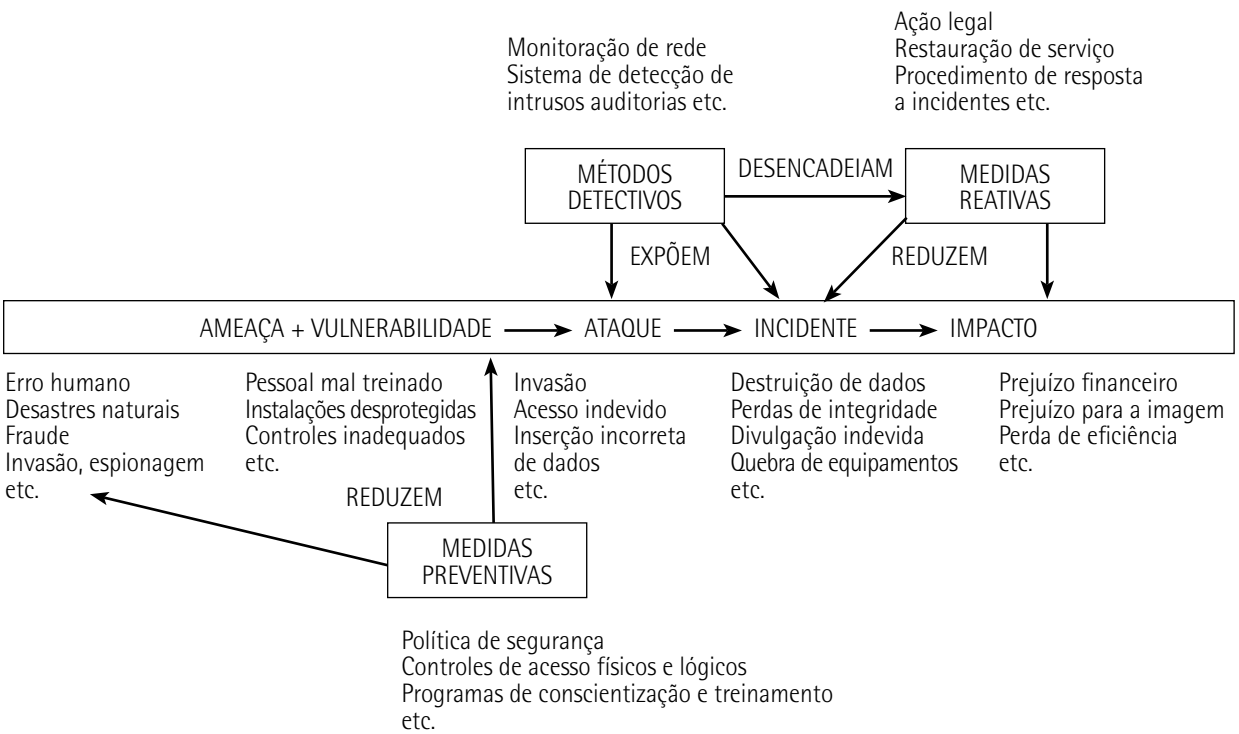

Figura 12 – Componentes de riscos e medidas de proteção usadas para reduzi-lo

> Medidas preventivas são controles que reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente/ativo/sistema, reduzindo assim a probabilidade de um ataque (BEAL, 2008, p. 27).

Medidas corretivas ou reativas são as medidas normalmente tomadas após a ocorrência de um evento, com o objetivo de reduzir o impacto de um ataque/incidente.

Medidas detectivas expõem ataques/incidentes e disparam medidas reativas, com a intenção de evitar a concretização do dano, reduzi-lo ou impedir que volte a acontecer.

Diante de um risco é possível adotar medidas para tratar o risco ou reduzir suas consequências: evitar o risco significa não expor o ativo a situações de risco; transferir o risco significa fazer um seguro para cobrir prejuízos causados por algum impacto; reter significa fazer um autosseguro; reduzir significa implementar uma proteção que diminua o risco; e, por último, mitigar significa tomar medidas que diminuam apenas o impacto.

Observação

Um exemplo de medida de proteção que reduz a probabilidade de uma ameaça ocorrer seria a mudança física de um data center (alvo) por motivos de enchentes constantes na região.

Quadro 15 – Exemplos de medidas preventivas e reativas e de métodos detectivos para a proteção da informação

Ameaça	Medidas preventivas	Medidas reativas	Medidas detectivas
Fraude	Supervisão gerencial, segregação de funções, controle efetivo de senhas e permissões de acesso	Interrupções de pagamentos suspeitos, investigação interna, denúncia à polícia	Auditoria de *logs*, análise de trilhas de auditoria, conciliação de valores
Furto de equipamento	Controle de entrada e saída	Investigação interna, denúncia à polícia	Inventário periódico, controle de entrada e saída

Fonte: Beal, 2008, p. 28.

A terceira atividade se refere à aceitação do risco, que ocorre quando o custo de proteger um ativo em relação a um determinado risco simplesmente não vale o benefício. Isso ocorre quando os mecanismos de proteção excedem o valor do próprio ativo de informação ou então quanto os riscos que o ativo está correndo está dentro dos critérios de aceitação pela organização.

A aceitação de um risco não quer dizer que sua presença foi ignorada pela organização. Pelo contrário, sua presença é reconhecida e a decisão de aceitar o risco também é considerada uma forma de tratamento do risco.

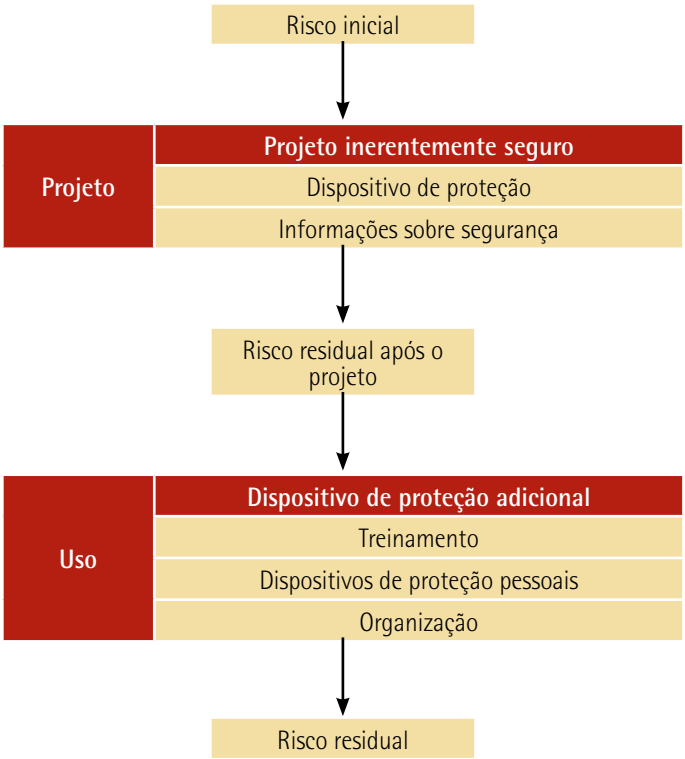

Figura 13 – Tratamento do risco.

Por último temos a comunicação do risco, que nada mais é do que divulgar as informações sobre os riscos que foram identificados, tratados ou não, para todas as partes envolvidas.

A comunicação dos riscos às partes envolvidas é uma forma de envolver ou criar responsabilidade em todos aqueles que efetivamente precisam cuidar dos ativos de informação. A melhor forma de comunicar os riscos é de forma genérica, para evitar a exposição e para que todos tenham informações sobre os riscos organizacionais.

2.2 Sistema de gestão de risco

Quando a palavra "gestão" é proferida, logo remetemos aos conceitos de administração, estratégia, processo decisório, ao passo que a palavra "sistema" remete, em sua essência, a um conjunto organizado que trabalha em prol de um resultado comum.

Podemos dizer que o sistema de gestão de risco é o ato de administrar o risco criando mecanismos para identificar, analisar, tratar e comunicar as decisões sobre as melhores formas de gerir esses riscos, alinhados com a estratégia da organização.

O conceito de gestão pressupõe que exista um planejamento de como o risco deve ser trabalhado, criando assim um modelo corporativo de gestão de riscos. Esse sistema deve também estar alinhado com os aspectos jurídicos e culturais, com as normas e com as práticas de mercado.

Os benefícios do uso sistemático de um programa de gestão de riscos são evidentes, pois, quando implantado e seguido com eficácia, as organizações, além de priorizar os riscos e suas ações, conseguem conhecer melhor os riscos e tomar conhecimento de quais mecanismos têm o consenso administrativo. Assim, terão maior embasamento para adotar proteções e terão uma métrica com indicadores de resultados realmente eficazes.

A introdução de um sistema de gestão de risco nas organizações é um processo trabalhoso que depende da cooperação de todos e da anuência da executiva da organização. Um dos maiores desafios é conseguir aperfeiçoar o tempo dos processos de gestão de risco sem deixar passar informações importantes, ao mesmo tempo em que é preciso maximizar os resultados.

Um ponto importante neste processo é a extrema dinamicidade que diversos ativos de informação possuem, principalmente os ativos tecnológicos, pois isso dificulta o processo de análise e, consequentemente, pode torná-la imprecisa.

Desafios estruturais também devem ser transpostos, como a escassez de informações estatísticas sobre os ativos de informação, mesmo que esses valores sejam qualitativos (muito alto, alto, médio, baixo etc.). O grande impacto para o sistema de gestão de riscos é que essa dificuldade afeta as estimativas de probabilidade e de impacto na análise de um evento.

Outro desafio estrutural reside no fato de que é muito difícil estabelecer uma estimativa de custos. Em geral, custos diretos em decorrência de um problema são relativamente fáceis de calcular, porém, os custos indiretos, como produtividade, imagem e mercado são extremamente complexos e às vezes totalmente imprecisos.

No entanto, apesar das dificuldades, a grande maioria dos especialistas em segurança da informação concorda que a implantação de um sistema de gestão de risco é fundamental para a organização de uma empresa.

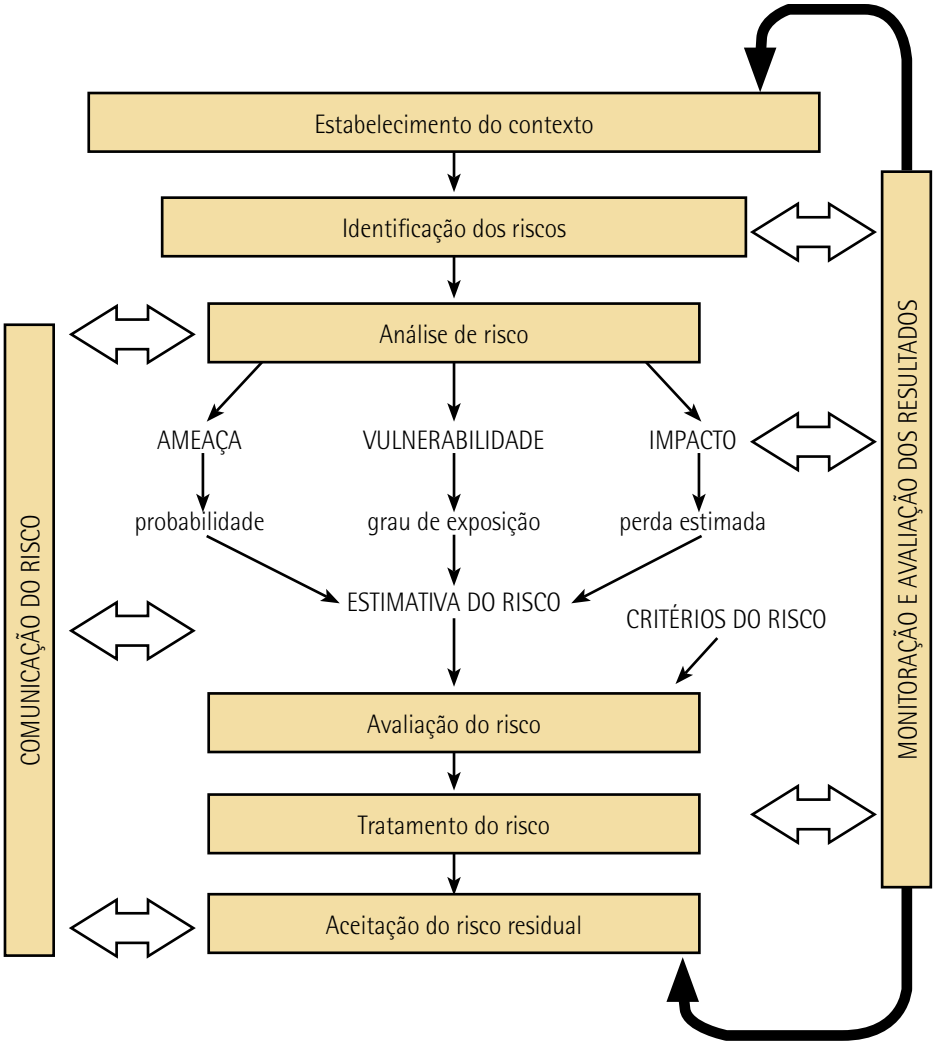

Figura 14 – Etapas da gestão de risco

2.3 Implantando o sistema de gestão de risco

Quando dizemos que a implantação de um sistema de gestão de risco deve ser tratada como um projeto de grande porte da organização, isso quer dizer que requer disciplina, planejamento, recursos e boa dose de jogo de cintura para lidar com os problemas que aparecerão no decorrer do projeto. Por esse e outros motivos, é recomendado que uma metodologia de gerenciamento de projetos seja seguida.

Assim, é aconselhável que cada organização respeite suas características, como cultura, disponibilidade de recursos, entre outras. Para a implantação de um sistema de gestão de riscos, é preciso seguir sete fases ou etapas, descritas a seguir:

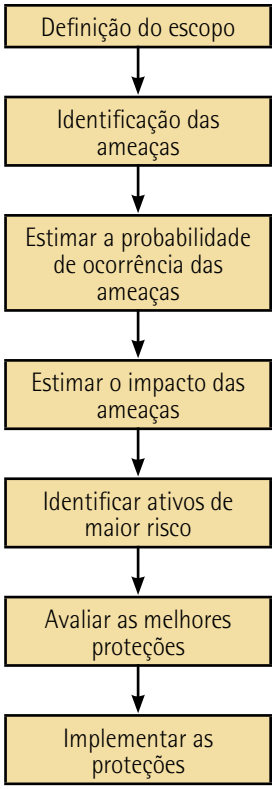

Figura 15 – Processos do sistema de gestão de riscos

Saiba mais

Os filmes a seguir podem propiciar uma breve noção, mesmo que fictícia, de uma análise e de uma gestão de riscos relacionadas com os conteúdos da unidade:

Onze homens e um segredo. Dir. Steven Soderbergh, 117 minutos, 2001.

Hitch - Conselheiro Amoroso. Dir. Andy Tennant, 105 minutos, 2005.

Primeiramente, todo projeto requer a definição de seu escopo, que geralmente é o fator mais importante para o sucesso de um projeto. Trata-se basicamente da definição da justificativa do projeto, do que será entregue ao final e, principalmente, dos limites do projeto.

No que tange à segurança da informação, o levantamento do escopo pode ser realizado por meio de entrevistas com gestores de processos e profissionais de segurança. O escopo precisa ser definido pela quantidade de ativos de informação que devem necessariamente ser agrupados em categorias para facilitar o processo, o qual, por sua vez, deve estar diretamente alinhado com a estratégia da organização e com os negócios que ela suporta.

É sabido que toda organização possui processos, uns mais críticos que outros, e que cabe aos seus gestores definir a importância de seus processos de negócios. Assim, a categorização por grupos pode ser visto sob diversos ângulos. Vejamos:

Quadro 16 – Formas de categorizar os ativos de informação

Categorização	Como é feito	Vantagens	Desvantagens
Por processo de negócio	Primeiramente é feito o mapeamento dos processos de negócio e, posteriormente, escolhemos os ativos que suportam cada um deles	Grande alinhamento da análise e avaliação de risco com o negócio da empresa, já que os ativos são selecionados de acordo com os processos mais importantes	Impossível de ser executado caso a empresa não possua os processos mapeados
Por localidade física	Selecionam-se todos os ativos constantes em um local	O levantamento de ativos pode ser feito de forma bastante rápida	Não há alinhamento da lista de ativos com os processos de negócio
Por tipo de ativo	Dá-se o foco a ativos de um determinado tipo, geralmente ativos de TI	Especialmente eficaz quando a análise e a avaliação de risco são feitas pelo departamento de TI da empresa e tem foco predominantemente técnico	Negligencia ativos importantes pelo simples fato de eles não se enquadrarem na questão, levando a um alinhamento menor com o negócio
Mista	Combinam-se os critérios acima de acordo com a necessidade	Varia de acordo com a abordagem	Varia de acordo com a abordagem

A definição do escopo também inclui o plano de trabalho a ser seguido, o qual engloba cronogramas, alocação de recursos e orçamentos.

Após definido o escopo é necessário identificar as possíveis ameaças às quais estão sujeitos cada ativo. Essa fase é crítica, uma vez que grande parte dos profissionais procura trabalhar com uma lista completa, além de iniciar uma busca indeterminada e interminável na internet de todos os aspectos possíveis, razão pela qual é necessário tomar alguns cuidados.

Também é importante notar que é necessário trabalhar com ameaças genéricas, ou seja, em vez de relacionar uma infinidade de ameaças, é mais simples trabalhar com a indisponibilidade de sistema (erro de usuário, falha de sistema, contaminação por vírus, entre outros problemas). Dessa maneira, os problemas de indisponibilidade serão tratados de forma semelhante.

Como o número de ameaças que pode assolar um ativo é infinito, é imprescindível que o profissional se concentre nas ameaças mais comuns, que comprovadamente representam aproximadamente 80% dos casos de incidentes de segurança, em termos de volume.

A utilização de listas prontas de possíveis ameaças é um recurso válido, uma vez que criar uma lista própria é um trabalho bastante extenso que demanda tempo e pessoal habilitado. Por essa razão, é bem mais simples e barato utilizar listas elaboradas e mantidas por grupos de pesquisa, institutos e comunidades, ou que são inseridas em *softwares* de gestão de riscos.

O passo seguinte é **estimar a probabilidade de ocorrência das ameaças**. Logo após o mapeamento das ameaças é necessário avaliar a probabilidade de que elas venham a ocorrer. A probabilidade pode ser avaliada a partir de dois fatores: a frequência e a vulnerabilidade.

- **Frequência:** representa a quantidade esperada de vezes que uma ameaça tente causar algum dano a um ativo. Independentemente de quantas vezes uma ameaça tente causar algum dano, ela somente terá êxito caso consiga explorar alguma vulnerabilidade.

- **Vulnerabilidade:** conforme definido anteriormente, é a ausência de mecanismos de proteção ou uma falha em um mecanismo de proteção existente. Para analisar as vulnerabilidades é necessário identificar as falhas ou ausências de proteção para um determinado ativo, porém não se trata de uma tarefa fácil, principalmente para os componentes de tecnologia da informação (TI). Para esses componentes é recomendado o uso de ferramentas automatizadas que possam realizar a captura de vulnerabilidades. Dentre essas ferramentas, algumas possuem listas de pontos de verificação para os ativos.

Seguindo o processo de implantação da gestão de riscos, temos a etapa de **estimação do impacto das ameaças**, que se refere à avaliação do impacto que a concretização de uma ameaça vai causar naquele determinado ativo. Diferentes ameaças causam diferentes impactos, porém, quanto maior o número de ameaças, maior será o risco. Inclusive, além do impacto, o valor do ativo de informação para a organização também deve ser levado em consideração, valor esse que é demonstrado pelo ser valor absoluto (como o preço para adquirir outro igual) ou relativo (associado ao benefício que aquele ativo traz).

Estimado o impacto das ameaças, é necessário identificar os ativos de maior risco. Nesse momento, estão devidamente documentados os processos de negócio, as ameaças aos quais os ativos estão sujeitos e a probabilidade de as ameaças se concretizarem por conta de sua frequência e vulnerabilidades existentes – assim, estão preparados os componentes para o cálculo do risco.

Nessa hora, os ativos que correm mais risco devem ser priorizados para a implantação dos mecanismos de proteção, porém isso não é uma regra, uma vez que as organizações, em razão do custo, podem optar por mecanismos secundários para ativos de maior importância. Esse método é adotado em razão da adição de mais um mecanismo para sanar uma vulnerabilidade em um mecanismo instalado que receberá apenas um complemento.

Devidamente identificados os ativos de maior risco ao qual uma determinada organização está sujeita, entramos na fase de avaliar as melhores proteções. Todo e qualquer profissional de segurança da informação sabe que todos os ativos de informação estão sujeitos a algum tipo de risco, porém é conhecido que os recursos destinados à proteção dos ativos de informação são limitados e que por vezes mal conseguem trazer os riscos identificados para os patamares aceitáveis, conforme estabelecido pelo critério de risco.

Como há uma escassez de recursos, os profissionais de segurança da informação são obrigados a priorizar os ativos de riscos maiores, o que vai depender de dois fatores:

1. **Disponibilidade dos recursos;**

2 **Eficácia no uso dos recursos disponíveis** – está relacionada à capacidade dos profissionais de segurança em escolher entre as proteções que tenham melhor custo-benefício.

Existem diversas formas para avaliar o custo-benefício das proteções a serem implantadas. Assim, podemos dividir o processo de implantação da seguinte maneira:

1. Primeiramente, estimativa do que a organização perderá em um ano, levando em consideração o impacto e a probabilidade de as ameaças se concretizarem.

2. Em seguida, avaliação das soluções disponíveis para resolver ou amenizar o problema. Essa fase, por sua vez, está dividida em três atividades:

   - Estimar as perdas às quais a organização está sujeita após a implementação da proteção, de forma que será conhecido exatamente o percentual do montante original que a proteção ajudará a reduzir;
   - Com o percentual bruto gerado, calcular o percentual líquido para um determinado período, levando em consideração os custos ligados à implementação da ferramenta;
   - Ligada ao percentual líquido que, depois de gerido, possibilita a identificação exata de quanto será o aporte financeiro inicial para a implementação da proteção. Caso o montante seja maior do que se espera economizar, o investimento no mecanismo de proteção será inviabilizado.

3. Implementação das proteções escolhidas. Logo após todas as checagens de "sanidade" para o investimento que será gasto na determinada proteção, ela é finalmente implementada.

4. Definição e monitoramento das métricas. É necessário averiguar se os mecanismos escolhidos e implementados estão realmente atingindo os índices de eficiência estipulados. Uma estimativa mal elaborada pode ter o resultado inverso, de modo que, em vez de proteger o ativo de informação, pode-se deixá-lo ainda mais vulnerável.

5. A última etapa do processo é a de implementar as proteções, que pode durar vários meses e demandar muitas atividades que afetarão o cotidiano da empresa. Pode ser necessária a abertura de novos projetos para a implantação de mecanismos de proteção em ativos de informação.

Observação

A implantação dos mecanismos de proteção pode interferir diretamente no cotidiano dos sistemas de uma organização, razão pela qual é recomendada a utilização de planos de teste, homologação e gerenciamento de mudanças para a conclusão do processo de implantação.

Resumo

A informação possui um papel fundamental dentro das empresas, seja qual for o processo no qual esteja envolvido. Por esse motivo, criar formas de proteger esse ativo é muito importante para a sobrevivência das organizações. Diante desse desafio, as áreas de tecnologia da informação (TI) assumem uma grande responsabilidade, uma vez que com a automatização dos processos empresarias as organizações passaram a depositar todas as suas informações em sistemas geridos e administrados pela tecnologia da informação.

No entanto, a segurança da informação não é composta apenas em protegê-las quando estão em sistemas automatizados, mas em estabelecer mecanismos que as protejam sob a esfera de três componentes básicos que norteiam todas as decisões referentes à segurança da informação:

- pessoas;
- processos;
- tecnologia.

Nessa esfera, podemos acrescentar que, diante dos componentes, temos os pilares que sustentam a proteção dos ativos de informação e que norteiam todas as ações para tal. São eles: a confidencialidade, a integridade, a disponibilidade, a legalidade e a legitimidade.

Podemos dizer que as informações têm vida, pois possuem um ciclo que precisamos compreender para, assim, reconhecer em quais momentos ela requer menos ou mais proteção.

O ciclo de vida da informação passa obrigatoriamente em algum momento por esses estágios: gerada, tratada, transmitida, armazenada e descartada.

Seria fácil para os gestores se adotassem mecanismos de proteção para todas as informações da empresa, porém proteger os ativos de informação é uma operação muito cara e trabalhosa. Então, como proteger os ativos que realmente são importantes para a organização e assim transformar a segurança da informação em um processo eficaz dentro da empresa?

A resposta para essa questão reside na classificação da informação, que na prática consiste em organizá-las pelo seu grau de importância

e, a partir daí, definir quais os níveis de proteção que cada ativo de informação requer. Dessa forma, evita-se a implantação desnecessária de mecanismos de proteção para ativos de pouca importância e também que sejam aplicados mecanismos inferiores para ativos sensíveis ou extremamente importantes, o que os deixaria vulneráveis.

Quando a empresa implanta o processo de classificação da informação, está preparada para estabelecer uma gestão de riscos eficaz. O processo de gestão de risco é responsável por identificar, avaliar e implementar medidas de proteções necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informações.

Por meio de análises, a gestão de riscos de uma empresa deve conhecer o cenário de risco ao qual cada ativo de informação está exposto diante da fase do ciclo de vida em que ele se encontra.

Uma ameaça visa a explorar uma vulnerabilidade do ativo de informação dentro do ambiente corporativo, sendo em processos, pessoas ou tecnologia. Após identificar seu alvo, a ameaça a partir do seu agente vai ao ataque, sempre tentando quebrar um dos pilares da segurança da informação, a confidencialidade, a integridade ou a disponibilidade do ativo, conseguindo assim causar impacto no ativo da informação-alvo.

A gestão de risco tem como missão identificar as vulnerabilidades e adotar mecanismos que tentem impedir que elas sejam exploradas, salientando que, em segurança da informação, falar em algo 100% seguro é utopia.

Diante de um cenário de risco, cabe aos gestores implantar medidas que visam a inibir a ação do agente e da ameaça. Isso é feito por meio de um processo que se inicia a partir da identificação, da análise, da estimativa do grau, da avaliação, do tratamento do risco e, por último, da aceitação do risco residual.

Exercícios

Questão 1. Idalgo Albert de Souza é um gestor consciente e preocupado com a segurança da informação na organização Armagedon Têxtil S.A., na qual atua como executivo de TI. Todavia, está ocorrendo constantemente vazamento de informações, o que coloca em risco a posição de mercado da organização. Indignado, Idalgo convocou a equipe de segurança da informação e questionou sobre o que poderia estar acontecendo na organização. Sua equipe respondeu que o problema poderia ser originado de algumas vulnerabilidades existentes.

Das afirmativas abaixo, identifique qual ou quais afirmativas estão corretas sobre as possíveis vulnerabilidades que podem permitir o vazamento de informações na Armagedon Têxtil S.A.

I. Os processos que, em algum momento, estão vulneráveis às ameaças.

II. A confidencialidade da informação que, de certa forma, sofreu alterações.

III. As pessoas que podem estar vulneráveis e de forma involuntária, ou até mesmo por má intenção, poderiam vender informações aos concorrentes.

IV. O uso incorreto das tecnologias disponíveis que poderiam abrir ou criar vulnerabilidades nos sistemas informatizados da empresa.

Assinale a alternativa correta:

A) Apenas as afirmativas I e II são verdadeiras.

B) Apenas as afirmativas II e III são verdadeiras.

C) Apenas as afirmativas II, III e IV são verdadeiras.

D) Apenas as afirmativas I, III e IV são verdadeiras.

E) As afirmativas I, II, III e IV são verdadeiras.

Resposta correta: alternativa D.

Comentário das afirmativas:

I. Afirmativa correta. Os processos são elementos a serem acompanhados pela área de segurança da informação e podem, em algum momento, estar vulneráveis.

II. Afirmativa incorreta. A confidencialidade da informação nunca pode ser a causa do vazamento de informações, pois é um dos pilares da segurança da informação. Outro ponto reside no fato de que a confidencialidade da informação pode ser quebrada e não alterada; o princípio que pode sofrer alterações é de integridade das informações.

III. Afirmativa correta. As pessoas são consideradas, dentro dos elementos de segurança da informação, o fator que pode oferecer as maiores vulnerabilidades à segurança da informação, tanto de forma intencional (referente à conduta fora da ética e criminosa) como de forma não intencional (por falta de conhecimento, treinamento ou até mesmo ingenuidade).

IV. Afirmativa correta. O uso da tecnologia de forma incorreta pode acarretar em sérios riscos à segurança da informação.

Questão 2. Idalgo não se sentia confortável com a situação apresentada e desafiou a equipe de segurança da informação, questionando sobre o que poderia ser realizado ou implantado para diminuir as vulnerabilidades existentes e assim conter, ou até mesmo prevenir, o problema de vazamento de informações na Armagedon Têxtil S.A.

Analise as propostas oferecidas pela equipe de segurança da informação, identificando a(s) opção(s) correta(s).

I. Entender o cenário através de avaliação de risco. Dessa forma, será possível identificar quais são as vulnerabilidades da organização e, assim, adotar mecanismos de proteção adequados às potenciais ameaças que podem explorar as vulnerabilidades existentes.

II. Adotar um plano organizado de classificação da informação para identificar os ativos de informação críticos para a organização e, assim, adotar os mecanismos de proteção corretos e eficazes, reduzindo os investimentos e evitando desperdícios.

III. Adotar um plano de conscientização para informar os colaboradores (as pessoas) sobre o seu papel na segurança da informação para que prestem mais atenção ao assunto e não deixem vulneráveis as informações sob sua responsabilidade.

IV. Implantar imediatamente um processo de auditoria nos acessos lógicos dos sistemas informatizados, verificando sua aderência às melhores práticas e regras da organização a fim de identificar qualquer tipo de vulnerabilidades ou possíveis vazamentos de informação.

Assinale a alternativa correta:

A) Apenas as afirmativas I e II são verdadeiras.

B) Apenas as afirmativas II e III são verdadeiras.

C) Apenas as afirmativas II, III e IV são verdadeiras.

D) Apenas as afirmativas I, III e IV são verdadeiras.

E) As afirmativas I, II, III e IV são verdadeiras.

Resolução desta questão na Plataforma.