Segurança em Sistemas de Informação

Fundamentos de Segurança da Informação

Aula 1

Prof. Luis Gonzaga de Paulo

Conversa inicial

No início da era da informação, em meados do século passado – e especialmente durante as grandes guerras que assolaram o mundo –, o armazenamento e o tráfego de informações eram algo muito restrito, porém o valor da informação já era considerado algo estratégico.

Com a evolução das comunicações e principalmente dos computadores, com o brutal incremento da capacidade de obtenção, processamento e movimentação da informação – principalmente no formato digital –, percebeu-se que este valor despertava o interesse e estava sujeito a diversas ameaças, necessitando de cuidados para sua preservação por meio do uso adequado.

O período denominado "Guerra Fria" foi o apogeu de temores quanto à perda de informações ou da sua obtenção por forças adversárias, impulsionando os estudos e o desenvolvimento de uma nova área de conhecimento dentro da computação: a de segurança da informação. Nos tempos atuais, da conectividade total, *mobile*, internet das coisas, *big data*, o conhecimento dessa área passou a ser determinante para os que atuam na indústria da computação, e é o que se pretende apresentar e desenvolver nesta aula.

Para saber mais, assista ao vídeo institucional sobre Segurança da Informação, produzido pela Coordenadoria de Auditoria em Tecnologia da Informação do Superior Tribunal de Justiça, disponível em:

https://www.youtube.com/watch?v=nVmRHtHJKfw

Para uma introdução da aula, assista ao vídeo que está disponível no material *on-line*!

Contextualizando

Você já observou a crescente preocupação das pessoas com a segurança da informação? A mídia retrata frequentemente os problemas de roubo, chantagens e divulgação de informações privativas e confidenciais, invasão de privacidade e muitos outros incidentes. Por que isso acontece? O que é possível

fazer para evitar tais incidentes? Podemos nos resguardar desses acontecimentos? Podemos proteger a informação e evitar que seja usada indevidamente? Como? São a essas respostas que pretendemos endereçar os estudos desta aula.

Para saber o que o professor Luis tem a dizer sobre o assunto, assista ao vídeo que está disponível no material *on-line*!

Antes de iniciarmos a apresentação do conteúdo, que tal pesquisar um pouco? Veja o conteúdo da Unidade 1 – "Um panorama da segurança da informação: definições e princípios básicos", do livro "Fundamentos em Segurança da Informação", da bibliografia básica da disciplina. Também é importante que, a partir de agora, você pesquise o tema "Sistemas de numeração" no Google, leia os artigos e textos disponibilizados em "Materiais complementares" das aulas no AVA e assista aos vídeos recomendados.

A informação

Vivemos na Era da Informação e produzimos, armazenamos e movemos diariamente uma quantidade incalculável de informação. Apesar da quantidade de informação ter passado por um grande impulso, a partir da invenção da imprensa, por Gutemberg, foi a partir do final do século XVIII, com a invenção da fotografia, seguida do telégrafo – que inaugurou a era das telecomunicações – que a quantidade de informação produzida, disponível e transportada ganhou tamanha proporção.

Porém, cabe aqui uma reflexão: o que é informação? Nomes, números, imagens e sons, sensações, enfim, tudo aquilo que podemos experimentar com nossos sentidos – e, além deles, com o uso da tecnologia – e que tenha algum uso, propósito, que possa ser utilizado por meio da razão ou da emoção. Tudo isso é informação. E tudo isso tem valor, seja um valor mensurável ou não.

Para a tecnologia da informação o conceito é diferenciado, a começar pela separação entre a informação e os dados. Dados são elementos, valores,

grandezas medidas e ainda por analisar ou processar por meio de recursos computacionais. Informações são os resultados desta análise ou processamento que, mediante processos e regras definidas, tornam-se inteligíveis e utilizáveis pelos seres humanos. Entretanto, ambos – dados ou informações – têm um valor intrínseco, requerendo um tratamento pelo qual possam manter sua utilidade e seu valor.

A norma ABNT NBR ISO/IEC 27002:2103 define informação como sendo um ativo – isto é, bem, patrimônio – da organização, de grande importância e valor, e que por isso necessita de proteção adequada. Para isso, deve-se considerar a informação em suas diversas formas e nos diversos meios utilizados para obter, armazenar, transportar e modificar a informação:

> O valor da informação vai além das palavras escritas, números e imagens: conhecimentos, conceito, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como os outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.

Como existe uma grande diversidade de informações no ambiente pessoal e no ambiente corporativo, é necessário classificar as informações, isto é, diferenciá-las em função de níveis e critérios específicos, por exemplo a sua natureza, o seu valor e seu grau de importância. Esses critérios e níveis podem definir o grau de sigilo e confidencialidade a ser aplicado à informação. É também em função desses critérios que serão definidos os mecanismos de controle e proteção às informações.

Certamente você já ouviu ou leu a respeito de informações **confidenciais**, **secretas**, de **caráter reservado** ou **público**. São exemplos de classificações para informações que determinam quem, quando e onde podem ter acesso, transportar ou modificar determinadas informações.

A informação também percorre um **ciclo de vida**, isto é, um período compreendido entre a criação ou origem da informação até o momento em que pode ser descartada. Durante esse ciclo de vida, a informação é manuseada,

manipulada ou tratada, podendo sofrer alterações desde que controladas, de modo a não perder seu valor. Também pode ser armazenada ou transportada – submetida a processos que, entretanto, não mudam seu significado ou valor. Nesse ciclo de vida a informação também está exposta a riscos – isto é, vulnerável - por exemplo o roubo, a perda ou a alteração indevida. Para evitar que isso ocorra é necessário proteger a informação e monitorar seu ciclo de vida por completo. Este é o principal objetivo da segurança da informação.

Figura 1 - Ciclo de vida da informação

Acesse o material *on-line* e assista ao vídeo que está disponível para você!

Segurança da Informação

Para que a informação possa atender a seus propósitos e à demanda de pessoas e organizações, é necessário preservá-la e manuseá-la adequadamente. A segurança da informação é a área de conhecimento humano que tem por finalidade planejar e operar processos, técnicas, ferramentas e mecanismos – não necessariamente tecnológicos – que possam prover a devida proteção à informação, mas não somente isso: devem preservar seu valor. E para tanto também deve garantir o uso correto e adequado da informação.

A palavra “segurança” tem significados distintos e por vezes até conflitantes, podendo referir-se a ameaças intencionais, como intrusões, ataques, perda e roubo de informações (*security*, em inglês). Pode ser referência a sistemas confiáveis, construídos para reagir perante as falhas do *software*, do *hardware* ou dos usuários (*reliability*, em inglês). Outro significado remete aos problemas causados aos negócios, ao meio ambiente, à infraestrutura ou até

mesmo acidentes que tenham impacto nas pessoas ou representem risco à vida (em inglês, *safety*). A segurança da informação abrange a todos esses aspectos.

De acordo com a norma ABNT NBR ISO/IEC 27002:2103:

> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação sejam atendidos.

Já foi mencionado que a informação está sujeita a riscos, seja no processo de produção e manuseio, seja no armazenamento ou em seu transporte por qualquer meio. Esses riscos são decorrência dos diversos fatores envolvidos nesses processos: pessoas, tecnologias, ambiente, fenômenos naturais e o próprio desgaste ou fadiga pelo uso.

Os incidentes, isto é, as ocorrências que transformam a possibilidade do risco em um acontecimento, um fato, podem comprometer uma ou mais das características da segurança da informação, geralmente referenciadas pelo acrônimo **CID: Confidencialidade, Integridade e Disponibilidade**. Estes são os aspectos básicos da segurança da informação. Geralmente são acrescidos mais dois atributos: a **autenticidade**, e a **irretratabilidade** ou **não repúdio**. Alguns autores acrescentam também a **legalidade**, a **privacidade** e a **auditabilidade**, enquanto os demais defendem que tais princípios estão incluídos nos três principais.

A **confidencialidade** diz respeito ao uso autorizado da informação, isto é, decorre da classificação da informação e do controle do acesso à mesma. A **integridade** refere-se à manutenção do valor e das características originais da informação ou sua atualização por meio de alterações permitidas, controladas e identificadas, evitando-se a alteração indevida ou a perda de valor. A **disponibilidade** implica em prover a informação a tempo, no meio adequado e no local em que for necessária. A **autenticidade** visa garantir que a informação é real, verdadeira, legal e legítima, fazendo com que se possa confiar nela.

Irretratabilidade ou **não repúdio** objetiva garantir a autoria e a responsabilidade pela informação e pelo seu manuseio, evitando que possa haver negativa ou revogação de ações promovidas com a informação.

Figura 2 - A tríade das características básicas da Segurança da Informação

A segurança da informação compreende áreas distintas e interdependentes entre si, cuja ênfase estará relacionada diretamente com o negócio da organização. Essas áreas são:

- A segurança física, cuidando do acesso de pessoas aos locais e à infraestrutura de suporte à informação, delimitando o perímetro e utilizando dispositivos de alerta e proteção contra eventos naturais ou incidentes provocados pelos seres vivos em geral;
- A segurança da infraestrutura que suporta a informação, incluindo, mas não se limitando à energia, computadores, redes, dispositivos de armazenamento e transporte;
- A segurança do *software*, às vezes denominada segurança lógica, que responde às ameaças e riscos que afetam os programas de computador – incluindo-se o sistema operacional e o *software* de rede, sistemas de autenticação e criptografia, segurança no processo de desenvolvimento, na aquisição e na manutenção e atualização do *software*

O professor Luis traz mais explicações no vídeo que está disponível no material *on-line*!

Proteção da informação

Os procedimentos que buscam dar à informação a necessária e devida proteção compreendem um vasto arsenal de processos, mecanismos, técnicas, métodos e ferramentas que permeiam os três níveis da organização: estratégico, tático e operacional. Essa proteção está diretamente relacionada com o entendimento e comprometimento de todos os envolvidos, direta ou indiretamente, com o negócio da organização. Isso é um princípio básico da segurança da informação: a organização estará segura à medida que todos os que dela fazem parte – ou se relacionam com ela no desempenho de suas atividades – estiverem protegidos e se submeterem aos procedimentos de segurança.

Para isso a organização deve dispor de uma **Política de Segurança** que estabeleça claramente os objetivos a serem alcançados, o grau de tolerância ao risco aceitável para o negócio, e que oriente e norteie todas as iniciativas da organização relativas à segurança da informação. E, atenção: é de primordial importância que **todos**, na organização, tenham conhecimento dessa **Política de Segurança**, comprometam-se e atuem para colocá-la em prática e torná-la efetiva.

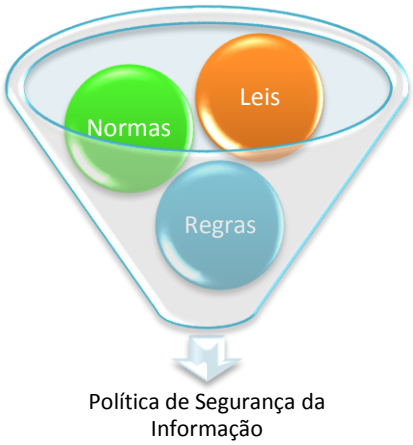
A Política de Segurança da informação deve estar submetida à **legislação**, alinhada com as práticas de **governança corporativa** e adequada às **normas** e **regulamentos** aos quais a organização está sujeita. A este aspecto denominamos *compliance* ou conformidade, o que deve ser aferido através de processos de certificação e/ou auditorias e torna a organização digna de confiança por parte dos governos, das outras organizações e do público em geral.

A Política de Segurança da informação também estabelece a hierarquia e as responsabilidades pela segurança da informação da organização, levando em conta que a segurança da informação não é responsabilidade exclusiva da área

de tecnologia da informação, comunicação e sistemas (TICS) e tampouco restrita aos aspectos tecnológicos.

Derivam dessa política e, portanto, devem ser compatíveis com ela as normas internas, os regramentos e os procedimentos operacionais que visam a manter a segurança da informação nos níveis adequados ao negócio da organização. Esses conjuntos de ordenamentos consideram as pessoas, os processos e as tecnologias envolvidas no ciclo de vida da informação, estabelecendo objetivos e critérios claros e compatíveis, além de mensuráveis e verificáveis, para que possam ser auditados e submetidos a processos de melhoria contínua, uma vez que a informação e os mecanismos que a suportam estão em constante processo de evolução.

Figura 3 – O embasamento da política de segurança da informação



Quer saber mais? Então acesse o material *on-line* e assista ao vídeo que o professor Luis preparou para você!

Vulnerabilidades e risco

A informação, como já visto, é um valioso ativo, isto é, um bem ou patrimônio da organização. Porém, para fazer uso desse valioso bem de forma a empregá-lo adequadamente ao processo produtivo da organização, é necessário prover meios para interagir com a informação no seu ciclo de vida.

Esses meios são os ativos da informação ou da tecnologia da informação (TI). Esses ativos compreendem uma vasta gama de dispositivos, equipamentos e componentes, desde os circuitos de comunicação de dados até o *software* (os programas), passando por redes, armazenamento, computadores e periféricos.

Cada ativo está sujeito a incidentes que podem influenciar na segurança da informação, seja pelo seu uso intenso, por se tratar de uma nova tecnologia cuja efetividade na segurança da informação ainda não foi comprovada, seja por haver interesses escusos devido ao alto valor. Enfim, tais ativos estão expostos a falhas de segurança da informação, possuindo pontos fracos que podem vir a ser explorados ou apresentarem comportamento incompatível, fraquezas, às quais denominamos **vulnerabilidades**. Ou seja, vulnerabilidades são pontos fracos nos ativos da informação que podem ser explorados ou apresentar falhas, gerando incidentes de segurança da informação.

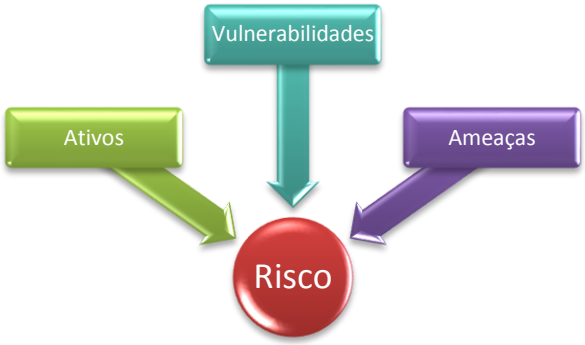
Além disso, estendendo o conceito de ativos às pessoas e processos da organização que atuam no ciclo de vida da informação, é possível afirmar que esses elementos também apresentam vulnerabilidades. Isso porque um suborno, a corrupção, omissão ou ação proposital podem gerar incidentes de segurança da informação, ou seja, pessoas e processos também apresentam vulnerabilidades.

As **ameaças** são agentes ou eventos que, podendo explorar ou agir perante uma vulnerabilidade, representam um **risco**. Para evitar incidentes de segurança da informação a organização necessita conhecer e gerenciar seus ativos (incluindo-se entre estes as informações de valor) e as vulnerabilidades destes. O processo de identificação e avaliação dos ativos, *asset assessment* ou inventário, deve então identificar, descrever e localizar cada ativo, seu uso e controles de segurança atuais e as ameaças às quais estão expostos ou submetidos.

Figura 4 – Os ativos da informação perante a segurança

O **risco** é a probabilidade de que uma ameaça venha a explorar ou agir contra uma vulnerabilidade, gerando um incidente de segurança da informação. Através de registros históricos, da análise matemática ou estatística, é possível determinar a probabilidade da ocorrência do risco e o impacto que esta ocorrência, ou incidente, pode causar nos negócios. Ao processo de avaliação de riscos executado desta maneira denomina-se **análise de riscos**.

Figura 5 – Os elementos do risco



A análise de riscos parte, então, de um inventário de ativos e, aplicando estudos, históricos e análise estatística, produz um panorama no qual são apresentados as probabilidades e os impactos dos riscos aos quais a segurança da informação está submetida. Essa análise é parte imprescindível do processo de **Gestão de Riscos** e pode partir dos seguintes questionamentos:

1. **Vulnerabilidade:** como a ameaça pode concretizar-se?
2. **Controle:** o que impede ou reduz a ocorrência atualmente?
3. **Ameaça:** o que se teme que possa acontecer?

4. **Ativo:** o que se pretende proteger?
5. **Probabilidade:** quais as chances de acontecer um incidente?
6. **Impacto:** qual o resultado do incidente nos negócios?

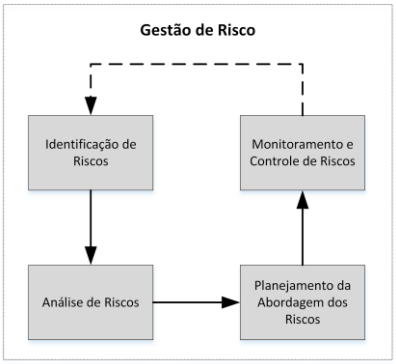
Figura 6 - A análise de riscos

Vamos aprofundar mais nossos conhecimentos? Então, assista ao vídeo que está disponível no material *on-line*!

Gestão de riscos

A **gestão de riscos** é um processo de suma importância para a segurança da informação. Pode-se considerar quatro atividades essenciais a esse processo, dispostas de forma sequencial e executadas de maneira cíclica, com base no modelo PDCA (*Plan, Do, Check, Act* ou seja, planejar, fazer, avaliar, corrigir).

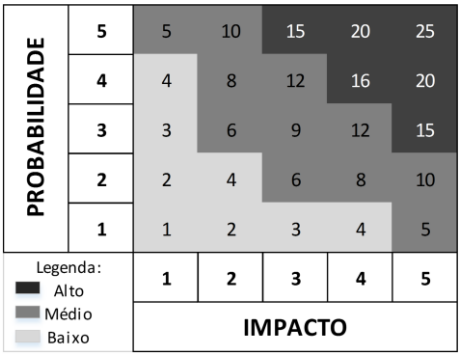
Figura 7 – O processo de gestão de riscos



Fonte: adaptado de PMBOK GUIDE (2013).

A atividade inicial envolve o planejamento e, para que seja efetivo, é necessário partir do inventário de ativos e promover a análise de riscos. É possível fazer a análise **quantitativa** do risco, construindo uma matriz PxI – probabilidade X impacto, que permitirá uma classificação do risco em função da combinação desses dois elementos. Uma outra abordagem é a análise **qualitativa**, que implica em atribuir um valor financeiro para o risco e assim estabelecer uma prioridade para o tratamento. Apesar de mais complexa, essa abordagem permite uma visão mais clara para a tomada de decisão, possibilitando inclusive o cálculo do **ROI** (*Return of Investment* ou Retorno do Investimento).

Figura 8 – A matriz PxI



Fonte: adaptado de Revista Contabilidade e Finanças (2007).

Uma vez identificados e analisados os riscos, são estabelecidas as estratégias de segurança da informação e então definidos e aplicados os controles, mecanismos de proteção e defesa. Ou seja, aplica-se o tratamento dos riscos com o intuito de mitigá-los.

As opções para o tratamento dos riscos são basicamente as seguintes:

- **Reduzir:** utilização de controles que reduzam a probabilidade ou o impacto do risco;
- **Reter ou evitar:** utilização de medidas que impeçam a ocorrência do risco pela eliminação de vulnerabilidades ou tratamento contra as ameaças, como a modificação ou substituição dos elementos

que apresentam vulnerabilidades ou o uso de alternativas mais seguras;

- **Transferir:** indicação de terceiros para adotar as providências para a mitigação do risco ou a administração das consequências;
- **Aceitar:** mesmo aplicando um tratamento aos riscos é improvável que se consiga eliminá-los totalmente. Sempre haverá um risco residual, por menor que seja, que fará parte do processo de aceitação do risco, dada a sua inexorabilidade ou a inviabilidade técnica ou financeira do tratamento. Essa aceitação deve ser comunicada e documentada para tornar-se de conhecimento de todos na organização.

Finalmente são necessários o monitoramento e a revisão da análise de riscos após a implementação do tratamento dos riscos. Isso se deve ao fato de que os riscos não são estáticos, uma vez que as ameaças, vulnerabilidades, probabilidades e o impacto podem mudar – e mudam – com o passar do tempo.

Podem ocorrer mudanças internas e externas à organização, na legislação, nas necessidades de segurança e no cenário ou ambiente da informação, os quais vão alterar os riscos. Também é necessário confrontar os riscos com as medidas adotadas para o tratamento deles, a fim de aferir a efetividade das mesmas. Por isso é necessário revisitar e revisar a análise de riscos de forma cíclica e recorrente e também atualizar as informações a respeito de novos riscos identificados e tratados.

Para finalizar os estudos deste tema, assista ao vídeo que está disponível no material *on-line*!

Trocando ideias

Acesse o fórum “Segurança da Informação” no Ambiente Virtual de Aprendizagem e converse com seus colegas de turma, tendo como premissa os seguintes questionamentos:

1. A segurança da informação é, atualmente, uma prioridade nas organizações?
2. Qual o impacto ou as consequências da falta de segurança da informação?
3. A gestão de riscos é praticada de forma adequada no ambiente de TI das organizações? Por quê?

Na prática

Para avaliar e aplicar seus conhecimentos, acesse no material complementar da disciplina no Ambiente Virtual de Aprendizagem o artigo "Gestão de Riscos". Pesquise na internet uma ocorrência de incidente de segurança recente e procure elaborar uma análise de riscos aplicável à situação relatada. Execute os seguintes passos:

1. Faça a leitura do artigo e anote os pontos que considerar importantes;
2. Leia a matéria a respeito do incidente de segurança que você identificou na mídia;
3. Pesquise casos semelhantes e principalmente quais foram as medidas corretivas adotadas;
4. Leia nas referências bibliográficas – especialmente nos livros indicados da Biblioteca Virtual – os temas relativos a riscos;
5. Elabore uma análise de riscos identificando os ativos envolvidos, os processos do negócio, as ameaças e os impactos;
6. Apresente suas conclusões e avalie a de seus colegas no fórum "Gestão de Riscos" da disciplina, no Ambiente Virtual de Aprendizagem;
7. Em caso de dúvidas ou dificuldades faça uso do canal de Tutoria do Ambiente Virtual de Aprendizagem.

Síntese

Nesta aula foram abordados alguns conceitos básicos da segurança da informação que permitirão desenvolver adequadamente o tema durante as aulas da disciplina. Foram tratados os aspectos da informação e de seu valor, a necessidade da proteção, as vulnerabilidades e riscos que afetam a segurança da informação e a gestão de riscos.

Para as considerações finais do professor Luis, assista ao vídeo que está disponível no material *on-line*!

Referências

GALVÃO, M. da C. **Fundamentos em segurança da informação.** São Paulo: Pearson Education, 2015.

ISO 27002:2013. **Segurança da Informação** – Coletânea eletrônica. Rio de Janeiro: ABNT, 2014.

PAULO, W. L. de; FERNANDES, F. C.; RODRIGUES, L. G. B.; EIDIT, J. Riscos e controles internos: uma metodologia de mensuração dos níveis de controle de riscos empresariais. **Revista Contabilidade e Finanças**, Vol.18, nº 43, USP, São Paulo, Jan/Abr, 2007.

PMI. **A Guide to the Project Management Body of Knowledgement (PMBOK GUIDE).** Project Management Institute, 2013.