Segurança em Sistemas da Informação

A Organização da Segurança da Informação

Aula 2

Prof. Luis Gonzaga de Paulo

Conversa inicial

Os processos que fazem parte da segurança da informação abrangem diversas áreas do conhecimento humano, estendendo-se também por toda a organização e permeando todos os processos e atividades que compõem o negócio. Devido a essa extensão, tem-se a impressão de uma grande complexidade, o que resulta em uma mistificação e distanciamento do tema, fato prejudicial aos objetivos da segurança da informação.

Na busca por mais segurança da informação e dos sistemas computacionais que tratam tais informações, é imprescindível conhecer todos esses processos para desmistificar o assunto, torná-lo simples e corrente entre as pessoas da organização, usuários de sistemas e serviços e o público em geral. Uma boa forma de fazer isso é conhecer o arcabouço legal que ampara a segurança da informação, os padrões, normas, regras, diretrizes, as boas práticas e todos os guias desenvolvidos e aprimorados no decorrer dos anos e que amparam os profissionais de TI e das demais áreas do conhecimento na busca por mais segurança da informação e dos sistemas. Nesta aula, pretende-se apresentar esses assuntos e assim desenvolver o conhecimento necessário para embasar a correta aplicação da segurança da informação e dos sistemas às organizações.

Para saber mais, assista ao vídeo institucional sobre Segurança da Informação, produzido pela Divisão de Segurança da Informação da Empresa Brasileira de Correios e Telégrafos, disponível em:

https://www.youtube.com/watch?v=xIPgmCGX7i4

Acesse o material *on-line* e assista ao vídeo de introdução da aula!

Contextualizando

Você já notou que a área de Segurança da Informação e de Sistemas é bastante abrangente e não diz respeito somente à Tecnologia da Informação, correto? Então, o que mais é necessário conhecer para proteger esse valioso

ativo da organização e das pessoas: a informação? Como endereçar as respostas corretas para a crescente demanda de segurança da informação e dos sistemas? O que deve ser levado em consideração ao iniciar um processo com vistas à garantia da segurança da informação e dos sistemas em uma organização? A quem recorrer para evitar a "reinvenção da roda" ou a adoção de medidas sem efetividade ou que possam causar problemas? Nesta aula, vamos abordar os temas pertinentes a estas e demais questões que surgem quando o tema segurança da informação e de sistemas é tratado.

Saiba o que mais o professor Luis tem a dizer sobre o assunto no vídeo que está disponível no material *on-line*!

Antes de iniciarmos a apresentação do conteúdo, que tal pesquisar um pouco? Leia os conteúdos das Unidade 2 e 4 do livro "Fundamentos em Segurança da Informação", da bibliografia básica da disciplina. Também é importante que, a partir de agora, você pesquise o tema "Segurança da Informação, Normas, Legislação" no Google, leia os artigos e textos disponibilizados em "Materiais complementares" das aulas no AVA e assista aos vídeos recomendados.

Marcos regulatórios

A necessidade de prover a segurança da informação e dos sistemas para assim preservar o valor da informação para as organizações e os indivíduos deve deixar-se conduzir pelos aspectos da legalidade, boa governança e *compliance*. Isso quer dizer que existem regramentos nacionais e internacionais que governam e servem de base para a definição e a aplicação das práticas de segurança da informação e de sistemas. Isso também implica em um aspecto de grande importância: a legalidade dessas medidas. Essa questão é de tamanha importância que alguns autores chegam mesmo a considerar a legalidade como um dos pilares da segurança da informação e dos sistemas.

Em termos globais uma referência aos marcos regulatórios que afetam a segurança da informação são as normas ISO/IEC, notadamente as da série 27000 (ABNT, 2014). A ISO (*International Standard Organization* ou Organização Internacional para a Padronização) é uma entidade com sede em Genebra, na Suíça, que reúne os órgãos nacionais de padrões, como a ABNT (do Brasil), a DIN (Alemanha) e a ANSI (dos Estados Unidos) de mais de 170 países.

O maior impacto global na segurança da informação e de sistemas foi gerado pela lei SOX (*Sarbanes Oxley*), promulgada em 2002 pelo Senado dos Estados Unidos. É uma lei voltada para as finanças, decorrente de problemas financeiros causados à economia mundial devido a fraudes contábeis, notadamente da companhia Enron com a cumplicidade da Arthur Andersen. Estabelece a criação de mecanismos de auditoria e segurança com base na governança e responsabiliza civil e criminalmente os gestores das organizações no caso de falhas. Mas por que uma lei norte-americana causou impacto no mundo todo? Primeiramente porque obrigou a todas as empresas que negociam suas ações nas bolsas de Nova York (NYSE - *New York Stock Exchange* e NASDAQ - *National Association of Securities Dealers Automated Quotations*) a submeterem-se aos seus rígidos mecanismos de controle. E, por conseguinte, essas empresas passaram a obrigar seus parceiros de negócio a tais mecanismos também, estabelecendo assim uma cadeia de responsabilidade de alcance mundial. Afinal de contas, nenhuma empresa pode sentir-se segura sozinha em um mundo globalizado e especialmente conectado pela tecnologia da informação e comunicações (TIC).

Outros marcos importantes que geraram impacto global:

- **HIPAA** (*Health Insurance Portability and Accountability Act* ou Lei de Portabilidade e Responsabilidade de Seguros de Saúde), que estabelece regras para a proteção das informações de usuários de planos de saúde nos Estados Unidos, gerando um modelo global neste sentido para as organizações da área de saúde;

- **FISMA** (*Federal Information Security Management Act* ou Lei de Gerenciamento da Segurança da Informação Federal) é uma lei dos Estados Unidos que regulamenta a segurança da informação dos sistemas de informação dos órgãos federais, aplicando-se a todos os sistemas de informação utilizados ou operados por agências, prestadores de serviço ou organizações vinculadas ao governo dos EUA (FISMA, 2013);
- **IFRS** (*International Financial Reporting Standards* ou Padrão Internacional para Relatórios Financeiros) é um conjunto de recomendações do IASB (*International Accounting Standards Board* ou Comitê Internacional de Padrões Contábeis) que estabelece padrões para o tratamento e publicação de informações financeiras e contábeis, adotado principalmente por bancos, financeiras, seguradoras e agentes do mercado financeiro;
- Os acordos de **Basiléia I, II e III**, atos de compromisso dos bancos centrais de diversos países para resguardar os clientes e os mercados dos riscos devido a problemas com bancos em geral. Como parte do complexo mecanismo de autorregulamentação, estabelece princípios de governança, transparência e auditoria, com impacto direto na segurança da informação e de sistemas.

No Brasil o tema tem a premissa constitucional como base. O Título II, Capítulo I, Artigo 5º (Casa Civil, 2016) trata do assunto em seus incisos, de maneira ampla e geral, a saber:

- V – é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
- IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
- X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

- XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (Regulamentado pela Lei nº 9.296, de 1996);
- XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
- XXVIII – são assegurados, nos termos da lei:
  - **a.** A proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas;
- XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (Regulamentado pela Lei nº 12.527, de 2011).

A partir desses estatutos foram criados diversos diplomas legais, entre os quais:

- **MP** (medida provisória) **2.200-2/2001**, que instituiu a ICP-Brasil (Infraestrutura de Chaves Públicas), iniciando o uso da certificação digital e assinatura eletrônica de documentos;
- **Decreto 3.714/2001**, que versa sobre a remessa eletrônica de documentos;
- **MP 2.026-7**, que instituiu a modalidade de compras por meio de pregão eletrônico;
- **Lei 9.609/98**, denominada “Lei do *Software*”, dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país etc.;

- **Lei 9.610/98**, a “Lei do Direito Autoral”, que altera, atualiza e consolida a legislação sobre direitos autorais;
- **Lei 12.737/12**, conhecida como “Lei Carolina Dieckmann” devido ao vazamento de fotos íntimas da atriz de mesmo nome na internet. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal;
- **Lei nº 12.965/14**, o **Marco Civil da Internet**, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Além desses, existem muitos outros textos legais que versam sobre a segurança da informação. Para ajudar no conhecimento da legislação aplicável, conheça o quadro resumo (DSIC, 2014) preparado pelo Depto. de Segurança da Informação e Comunicações da Casa Militar da Presidência da República, disponível no material complementar da aula.

O professor Luis fala mais sobre os marcos regulatórios da Segurança da Inforamação e dos Sistemas no vídeo que está disponível no material *on-line*!

Política de Segurança da Informação

A PSI (Política de Segurança da Informação) é um conjunto de orientações, regras, padrões e práticas que os membros da organização e aqueles que com ela se relacionam devem observar com vistas a garantir a segurança da informação adequada à organização.

Pode ser estruturada por meio de um ou mais documentos que contemplem aspectos normativos ou regulatórios, orientações e informações acerca das práticas de segurança da informação e de sistemas, do uso dos recursos, da hierarquia, estrutura e responsabilidades, das penalidades etc. Ou seja, a PSI é o dispositivo regulatório que deve embasar todas as atividades da organização que tenham relação com a segurança da informação e dos sistemas.

Como instrumento essencial, a PSI deve ser do conhecimento de todos – inclusive parceiros comerciais e clientes – e deve contemplar também os aspectos de formação e capacitação do pessoal, além da revisão cíclica e melhoramento contínuo, bem como processos de qualidade e auditoria para aferir o grau de efetividade de sua aplicação.

São referências importantes para a elaboração e manutenção da PSI:

- A devida fundamentação legal;
- O alinhamento com os negócios da organização;
- O uso de normas aplicáveis à segurança física, autenticação e controle de acesso à rede, sistemas, internet, e-mail, dispositivos móveis e de uso pessoal, recursos de TIC em geral, criptografia, aquisição, desenvolvimento e manutenção de *software*;
- Processo de divulgação, manutenção e revisão contínua para acompanhar evoluções e mudanças;
- Aceitação e conscientização;
- Verificação de conformidade e execução;
- Definição de procedimentos operacionais críticos, com admissão e demissão de pessoal, gerenciamento de crises: Quem faz? Como faz? Quando faz? Por que faz? Onde registra as alterações? A quem reporta as ocorrências?

Estes e diversos outros assuntos podem ser estruturados em processos e documentos à parte, que complementam a PSI. É importante que a PSI deixe claro que a segurança da informação e dos sistemas não é responsabilidade exclusiva da área de TIC, mas de todos.

Leitura obrigatória

Aprofunde seus conhecimentos com a leitura da Unidade 4 do livro “Fundamentos em Segurança da Informação”, da bibliografia básica da disciplina, item “Políticas e padrões de segurança”, pág. 100-104.

Para mais informações sobre a PSI (Política de Segurança da Informação), assista ao vídeo que está disponível no material *on-line*.

Estratégias de segurança da informação

Para tornar efetiva a PSI e estabelecer os controles corretos é necessário conhecer e adequar a organização às estratégias de segurança da informação e de defesa. Essas estratégias, ou grande parte delas, são oriundas de estratégias militares de defesa e foram validadas por sua aplicação por milhares de vezes no decorrer da história da humanidade. A seguir alguns exemplos:

- **Princípio do menor privilégio** implica em dar condições de acesso, ferramental e material minimamente suficiente para a execução das atividades pertinentes à função. Está ligada à ideia de hierarquia de privilégios e funções. Por exemplo, um operador de caixa de supermercado só pode realizar o registro das compras. Em caso de estorno ou cancelamento, um supervisor ou gerente tem que ser acionado.
- **Defesa em profundidade** significa prover diferentes mecanismos de forma combinada, de modo que são necessárias ações distintas para conseguir superar as defesas, que estão justapostas ou apresentadas em sequência ou diferentes níveis. Como exemplo, pode-se citar a fechadura da porta do carro, combinada com a chave de ignição e o sensor de presença da chave, muitas vezes também ligado ao alarme. São mecanismos bastante diferenciados com o único intuito de evitar o roubo do veículo, e que agem em sequência e em conjunto.
- **Ponto de estrangulamento** é a estratégia de reduzir ao mínimo indispensável os pontos de conexão e tráfego entre os ambientes internos e externos da organização, ou entre áreas de menor e maior proteção e segurança. E então aplica-se o maior contingente de medidas e mecanismos de segurança a este ponto, como o monitoramento, vigia, retenção e contenção, vistoria etc. A portaria

de um edifício, o portão de embarque no aeroporto ou o canal de comunicação de uma organização com a Internet são exemplos dessa estratégia.

- **O elo mais fraco** é o elemento de maior vulnerabilidade na escala de riscos e, portanto, requer a maior proteção. Pode ser também o elemento mais visado para eventuais ataques ou tentativas de uso indevido. Em segurança da informação e de sistemas é consenso que o elo mais fraco está associado a processos manuais ou que requeiram a intervenção humana, e também às próprias pessoas. Grande parte dos incidentes de segurança da informação estão associados às falhas ou iniciativas individuais e, geralmente, de pessoas ligadas às organizações vitimadas por tais ocorrências.
- **Posição à prova de falhas** corresponde à redução do perímetro de defesa para alvos de ataques em potencial, ou seja, os mais vulneráveis ou mais visados. Para essa posição são então direcionados os maiores esforços e recursos. São exemplos dessa estratégia os cofres das agências bancárias, os ambientes dos equipamentos do data center e os pontos de controle e observação, além de fontes de energia ou UTIs hospitalares.
- **Permissão ou negação padrão** é uma estratégia ligada ao controle de acesso e privilégios, ao monitoramento e ao processo de auditoria. Trata do uso de listas conhecidas como ***black list*** *ou* ***white list***. Uma *black list* é a relação de indivíduos, entidades, ações ou recursos com restrição ou proibição, devido ao conhecimento do risco em potencial que representam. Em síntese, uma *black list* é uma **relação de proibições** ou restrições, isto é, **do que não pode**. Já o oposto, a *white list*, é a lista sem restrições ou com as permissões, isto é, **do que pode**¸ normalmente aplicada quando o universo de possibilidades é difícil de se dimensionar. Um exemplo de *black list* é o código de trânsito, que estabelece os

comportamentos passíveis de punição. Já uma *white list* pode ser uma lista de convidados para um evento, quer seja, as pessoas que podem participar do evento.

- **Participação universal** é a estratégia de atuação em conjunto de todos os envolvidos nos processos de segurança da informação e dos sistemas. Implica em afirmar que nenhum processo ou iniciativa de segurança é suficientemente efetiva por si só e que o comprometimento de todos é o que reforça a efetividade das medidas. **A segurança da informação é compromisso e responsabilidade de todos!**
- **Diversidade da defesa** consiste em empregar mecanismos diferentes, no mesmo nível de proteção, reforçando os aspectos mais efetivos e reduzindo as deficiências de cada um. Um exemplo desta estratégia é o uso de uma cerca eletrificada, vigias humanos, cães de guarda e câmeras de monitoramento para controlar um perímetro de um edifício. Em TIC é comum esse tipo de estratégia utilizando *hardware, software* e processos específicos para prover a proteção desejada.
- **Simplicidade** é uma estratégia que prima pela facilidade do aprendizado e uso frequente. Além disso, uma segurança "ostensiva" pode causar o efeito indesejado de despertar o interesse justamente para os elementos mais capacitados e que oferecem maior risco. O ponto aqui é uma avaliação do tipo "se está com toda essa proteção então deve ter muito valor". A simplicidade não significa necessariamente uma solução simplista, improvisada ou fraca. Mas, sim, algo que possa ser colocado em ação rapidamente e por qualquer um, e por isso pode ser compreendido facilmente. Regras de composição de senhas, políticas de "*clear desk*" e "*clear screen*", descarte de impressos, atualização de *softwares* críticos como antivírus e a execução de

backups devem submeter-se a essa estratégia, sob pena de não serem executadas ou tornarem-se inócuas pela falta de uso.

- **Obscuridade** é a estratégia que prima pelo segredo, segundo o ditado que diz “o que os olhos não veem, o coração não sente”. Trata-se da ocultação de recursos, arquivos, técnicas usadas, versões de *software* e outros importantes referenciais que, obtidos com facilidade, dissimula ataques ou permitem uma ação mais direcionada e de maior risco. Uma das mais efetivas ações que buscam viabilizar ações escusas e ataques é a **Engenharia Social**, que deve ser enfrentada justamente por este tipo de estratégia.

Assista ao vídeo que está disponível no material *on-line p*ara mais informações sobre as estratégias de segurança.

Medidas de controle

Uma vez identificados os riscos e definidas as estratégias, é necessário prover, ativar e manter os controles, mecanismos e procedimentos que darão suporte a essas estratégias. Na área da TIC, isso engloba uma grande diversidade de elementos, controles físicos e lógicos que atuarão para garantir a segurança física e a segurança lógica, que podem ser minimamente diferenciados como:

- **Segurança física:** prevenção detecção e combate às ameaças físicas como incêndios, desabamentos, descargas elétricas, alagamento, acesso indevido de pessoas, forma inadequada de tratamento e manuseio dos ativos e da informação;

- **Segurança lógica:** prevenção, detecção e combate às ameaças "digitais" representadas principalmente por *malware*[1], acessos remotos à rede, *backups* desatualizados, violação de senhas etc.

Entre os mais diversos controles, mecanismos e procedimentos disponíveis e provavelmente utilizados pela organização estão:

- Identificação, autenticação e controle de acesso;
- Monitoramento, controle e auditoria de uso;
- Controles criptográficos, certificação digital e assinatura eletrônica;
- Antivírus, *firewalls*, proxies;
- Alarmes e sistemas de monitoramento, detecção e registro de tentativas ou ações de violação ou intrusão;
- Proteção da identidade ou garantia do anonimato;
- Cópias de segurança e sistemas de contingência e/ou tolerância a falhas.

Esses elementos, além da grande diversidade, são geralmente aplicáveis em conjunto e em diversas etapas do ciclo de vida da informação. Muitos deles fazem parte do mesmo conjunto de solução ou *appliance*. Porém, é imprescindível que sejam compatíveis com as estratégias de defesa e que estejam alinhados com a PSI e com o negócio. Caso contrário podem passar a incorporar novos riscos ou mesmo causar o efeito contrário ao desejado, além de comprometer os resultados da organização, causar repulsa nos indivíduos ou estimular a sabotagem ou as ações contra a segurança da informação e dos sistemas.

[1] Os *malwares* – do inglês, *Malicious Software*, são trechos de código ou *softwares* projetados para utilizar recursos computacionais de um dispositivo sem o conhecimento ou o consentimento de seu proprietário ou usuário habilitado (LA POLLA *et al.*, 2013). O propósito desse uso geralmente é ilegal ou desonesto, resultando invariavelmente em prejuízo.

Leitura obrigatória

Para aprofundar seus conhecimentos faça a leitura das Unidades 2 (releitura) e 3 do livro "Fundamentos em Segurança da Informação", da bibliografia básica da disciplina, item "Políticas e padrões de segurança", pág 27-85.

O professor Luis traz mais explicações sobre as medidas de controle. Assista ao vídeo que está disponível no material *on-line*!

Governança e *compliance*

Se uma organização prima por trilhar adequadamente os caminhos que levam à segurança da informação e dos sistemas, certamente terá adotado as boas práticas de **governança**, e estará ***compliance*** com a legislação, normas e regulamentos.

A governança compreende práticas de gestão que primam pela transparência, adequação às boas práticas e o reconhecimento, por parte do público externo – governo, fornecedores, clientes, mercado e consumidores – da organização como uma entidade confiável. É resultado de um esforço comprovado e contínuo para a melhoria dos processos, produtos e serviços, detecção, correção e antecipação dos problemas, do bom relacionamento e atendimento, da correta prestação de contas e garantia da confiabilidade. No plano da TIC e mais especificamente existem dois *frameworks* ou conjuntos de práticas que denotam este esforço: o **ITIL** e o **COBIT**. E diversas normas, mas em especial as do grupo **ABNT ISO/IEC 27000**, que, uma vez observadas e colocadas em prática, colaboraram para assegurar o atingimento das metas de segurança da informação e de sistemas.

O **ITIL** – *Information Technology Infrastructure Library* é um compêndio para orientar o gerenciamento mais eficiente da área de T.I., bem como para prestar serviços de maneira otimizada e eficaz. É também um conjunto de melhores práticas de gestão de T.I. que surgiu no final dos anos 80, com base em métodos criados pelo Governo Inglês, mais precisamente pela secretaria de

comércio (*Office of Government Commerce*, OGC). O ITIL como um padrão para o Gerenciamento de Serviços tem por finalidades:

- Promover a gestão mais eficiente da infraestrutura e dos serviços prestados pela área de TIC;
- Um maior controle nos processos e a minimização dos riscos envolvidos;
- A eliminação ou substituição pela unificação de tarefas redundantes;
- A definição clara e transparente de funções e responsabilidades da área de TIC;
- Uma melhoria contínua da qualidade dos serviços prestados;
- A flexibilidade e o controle da gestão de mudanças;
- A metrificação e a possibilidade de medir a qualidade;
- A redução de custos de TIC;
- A elevação dos indicadores da satisfação do cliente ou usuário;
- O provimento de respostas e processos mais ágeis;
- A comunicação mais efetiva, rápida e dirigida;
- A organização da área de TIC de maneira mais clara e sistemática;
- O uso de processos otimizados, consistentes e integrados/interligados;

O **COBIT** (*Control Objectives for Information and Related Technology*) é um conjunto de ferramentas que propõe o nível de excelência na gestão de TIC. É um guia para a gestão de TI recomendado pelo ISACA/ISACF (*Information Systems Audit and Control Foundation*), formatado para apoiar os gestores que necessitam constantemente avaliar o risco e controlar os investimentos de TIC em uma organização. Também destina-se aos usuários e clientes que precisam ter garantias de que os serviços de TIC – dos quais dependem os produtos e serviços internos e externos da organização – estão sendo bem gerenciados. E também serve de apoio para o pessoal de controle e auditoria, que podem se apoiar nas suas recomendações para avaliar o nível da gestão de TI e

aconselhar o controle interno da organização. O COBIT cobre quatro domínios pertencentes à área de TIC, quais sejam:

- Planejamento e organização;
- Aquisição e implementação;
- Entrega e suporte;
- Monitoração;

Juntamente com esses dois elementos, as normas ISO mencionadas podem prover as condições para que a organização esteja atuando em conformidade com as leis, as boas práticas e as recomendações de governança, isto é, esteja em ***compliance***.

Leitura obrigatória

Para saber mais, leia os artigos sobre Governança, ITIL, COBIT e o resumo das normas ISO aplicadas à Segurança da Informação disponíveis nos Materiais Complementares da disciplina.

E para tirar as dúvidas sobre governança e *compliance*, assista ao vídeo que o professor Luis preparou para você! Acesse o material *on-line*!

Trocando ideias

Acesse o fórum "Governança e *compliance*" no UNIVIRTUS e discuta com seus colegas de turma, tendo como premissa os seguintes questionamentos:

1. Qual é o estágio atual da aplicação do ITIL nas organizações que você conhece?
2. Como o COBIT pode colaborar com a segurança da informação e dos sistemas?
3. As normas ISO são conhecidas e aplicadas da forma adequada no ambiente de TIC das organizações? Por quê?

Na prática

Para avaliar e aplicar seus conhecimentos, avalie os ambientes que você frequenta (trabalho, escola, comércio, lazer etc.) quanto aos aspectos de segurança da informação, especialmente no que diz respeito às estratégias de segurança e medidas de controle.

1. Faça um levantamento e anote os pontos que considerar importantes;
2. Discuta com seus colegas no fórum “Análise da Organização da Segurança da Informação” e compare os levantamentos realizados;
3. Proponha melhorias ou mudanças nos pontos considerados;
4. Leia nas referências bibliográficas – especialmente nos livros indicados da Biblioteca Virtual – os temas relativos ao assunto para embasar sua proposta;
5. Apresente suas conclusões e avalie a de seus colegas no fórum “Análise da Organização da Segurança da Informação” da disciplina, no ambiente virtual de aprendizagem UNIVIRTUS;
6. Em caso de dúvidas ou dificuldades faça uso do canal de Tutoria do UNIVIRTUS.

Síntese

Nesta aula foram abordados os temas relativos à aplicação da Segurança da Informação e de Sistemas nas organizações, respeitando as leis, normas, regulamentos e boas práticas do mercado. Foram apresentados alguns dos principais marcos regulatórios, a política de segurança da informação e dos sistemas, as estratégias de segurança e as correspondentes medidas de controle e proteção, e finalmente os aspectos de governança e *compliance*. Complete ou refaça as leituras e as atividades recomendadas para reforçar seu conhecimento sobre estes temas.

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

Referências

Casa Civil. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em 20/02/2016.

DSIC. **Quadro da Legislação relacionada à Segurança da Informação e Comunicações**. Disponível em: http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm. Acesso em 20/02/2016.

PMI, a guide to the Project Management Body of Knowledgement (PMBOK GUIDE). Project Management Institute, 2013.

GALVÃO, M. da C. **Fundamentos em Segurança da Informação**. São Paulo: Pearson Education, 2015.

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

IFRS. **Informações – Termos Contábeis – IFRS**. Disponível em: http://www.contabeis.com.br/termos-contabeis/ifrs. Acesso em 10/02/2016.

FISMA. **Federal Information Security Management Act**. Disponível em: http://www.tiespecialistas.com.br/tag/fisma. Acesso de 10/02/2016.

LA POLLA, M.; MARTINELLI, F.; SGANDURRA, D. A. Survey on Security for Mobile Devices. **IEEE Communications Surveys & Tutorials**. Vol.15, Nº 1, First Quarter of 2013:446-471.

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.