Segurança da Informação e Proteção ao Conhecimento

Aula 12 – Conformidade

Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Conformidade

objetivos

Verificar a conformidade com políticas e normas de segurança da informação e avaliar a conformidade com a legislação.

conceitos

Legislação e direito digital no Brasil, verificação da conformidade com requisitos legais e auditoria.

Legislação e direito digital no Brasil

- Importância da legislação.
- Direito digital.
- Legislação e direito digital no Brasil.
- Direito digital e necessidades atuais.

Importância da legislação

Nas organizações, deve-se evitar o comprometimento e violação de:

- Leis criminais ou civis.
- Estatutos.
- Regulamentações.
- Obrigações contratuais.
- Requisitos de segurança da informação.

Os aspectos legais específicos devem ser considerados (legislação varia de acordo com o país).

Direito digital

Estabelece os princípios e instrumentos jurídicos que atendem à era digital, e envolve questões multidisciplinares:

- Civil.
- Trabalhista.
- Constitucional.
- Consumidor.

- Penal.
- Autoral.
- Contratual.

A seguir, são apresentados questionamentos exemplares relativos às questões tratadas na alçada do direito digital:

- **Questão civil**: a montagem de um website falsificado na internet, prejudicando determinada organização, pode ocasionar indenização por danos morais e materiais?
- **Questão trabalhista**: a demissão de um funcionário por mau uso de correio eletrônico é caracterizada como justa causa?
- **Questão constitucional**: o monitoramento do e-mail dos funcionários viola o direito à privacidade?
- **Questão do consumidor**: o compartilhamento de dados coletados na internet fere o Código de Defesa do Consumidor (CDC)?
- **Questão penal**: se um funcionário instalar programas piratas na máquina de trabalho, a empresa responde judicialmente?
- **Questão autoral**: a empresa tem direito aos códigos-fonte dos softwares que encomenda a terceiros?
- **Questão contratual**: os e-mails trocados entre as partes podem ser usados como prova de uma relação contratual?

Legislação e direito digital no Brasil

As leis não avançam a passos largos. Histórico:

- Código de Defesa do Consumidor, 1990.
- Propriedade Industrial – Lei 9.279, 1996.
- Constituição Federal, 1988.

- Propriedade Intelectual – Lei 9.610, 1998.
- Código Penal – Lei 9.983, 2000 – Lei 11.106, 2005.
- Código Civil, 2002/2003.
- Novas regulamentações – Sarbanes, Basiléia II e CVM 358, 2003/2004.

Legislação aplicável à segurança da informação

- Decreto 3.505, 13 de junho de 2000, do Poder Executivo, Artigos 1º e 3º.
- Artigo 5º da Constituição Federal.
- Lei 8.112/90, Inciso VIII do Artigo 116.
- Lei 9.609/98, Artigo 12.
- Código Penal, Artigos 307 e 308.
- Decreto 5.110, 2004.
- Decreto 5.244, 2004.
- PLC 35/2012 – Projeto de lei da Câmara dos Deputados que tipifica crimes cibernéticos.
- PL 2.126/11 – Proposta do marco civil da internet
- PLS 00481/2011 – Crimes de constrangimento e ameaça praticados nas redes sociais.

O Decreto 3.505, de 13 de junho de 2000 do Poder Executivo, em seu Artigo 3º, determina os objetivos da política da informação a serem aplicados nas organizações:

- IV – Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;
- V – Promover as ações necessárias à implementação e manutenção da segurança da informação.

O Artigo 5º da Constituição Federal determina em X: São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.

A Lei 8.112/90, inciso VIII do Artigo 116, determina: O servidor público tem o dever de guardar sigilo sobre assunto da repartição. E, no artigo 132, define a pena de demissão para o servidor que revelar segredo de que se apropriou em razão do cargo ou função.

A Lei 9.609/98 determina, no Artigo 12: Violar direitos de autor de programa de computador: pena de detenção de 6 meses a 2 anos ou multa.

O Código Penal determina, no Artigo 307: Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: pena de detenção de 3 meses a um ano ou multa. E no Artigo 308: Usar, como próprio, passaporte, título de eleitor ou qualquer documento de identidade alheia ou ceder a outrem, para que dele se utilize, próprio ou de terceiro: pena de detenção de 4 meses a 2 anos e multa.

O Decreto 5.110, de 2004, que acresce inciso ao Artigo 7 do Decreto 3.505/2000, institui a política de segurança da informação nos órgãos e entidades da administração pública.

O Decreto 5.244, de 2004, dispõe sobre a composição e o funcionamento do Conselho Nacional de Combate à Pirataria e Delitos Contra a Propriedade Intelectual e institui outras providências.

Decreto Nº 7.845, de 14 de novembro de 2012, que Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento (substituiu o Decreto 4553);

Links interessantes:

- **Imprensa Nacional**: www.in.gov.br
- **Presidência da República Federativa do Brasil – Legislação**: www.presidencia.gov.br/legislacao/
- **Legislação Específica Relacionada à Segurança da Informação**: http://dsic.planalto.gov.br/legislacaodsic/54
- **Documentos considerados sigilosos da Portaria nº 25, de 15 de maio de 2012**: http://sintse.tse.jus.br/documentos/2012/Mai/16/portaria-no-25-de-15-de-maio-de-2012-classifica

Exemplos de infrações digitais

A tabela seguinte apresenta exemplos de infrações digitais ocorridas em ambiente corporativo com a caracterização do crime e a legislação:

Conduta	Crime	Legislação	Pena
Enviar vírus, comando, instrução ou programa de computador que destrua equipamento ou dados eletrônicos.	Dano.	Art. 163, Cód. Penal	Detenção de 1 a 6 meses ou multa.
Publicar foto em rede de relacionamento contendo gestos ou imagens obscenas.	Ato obsceno.	Art. 233, Cód. Penal	Detenção de 3 meses a 1 ano ou multa.
Copiar um conteúdo sem mencionar a fonte; baixar MP3 ou filme, ilegalmente.	Violação de direito autoral.	Art. 184, Cód. Penal	Detenção de 3 meses a 1 ano ou multa (se a violação for com o intuito de lucro: reclusão de 1 a 4 anos e multa).
Criar uma comunidade virtual que ridicularize pessoas por conta de suas religiões.	Escárnio por motivo religioso.	Art. 208, Cód. Penal	Detenção de 1 mês a 1 ano ou multa.
Participar de comunidade virtual que discrimine pessoas por conta de sua etnia (por exemplo: "eu odeio nordestino", "eu odeio negros").	Discriminação por preconceito de raça, cor, etnia, religião ou procedência nacional.	Art. 20, Lei 7716/89	Reclusão de 1 a 3 anos e multa.

Conduta	Crime	Legislação	Pena
Enviar e-mail dizendo características negativas de uma pessoa (por exemplo: feia, gorda, ignorante, incompetente etc.).	Injúria (expor-se na internet pode virar difamação).	Art. 140, Cód. Penal Art. 139, Cód. Penal	Detenção de 1 a 6 meses ou multa. Detenção de 3 meses a 1 ano e multa.
Enviar e-mail a terceiros contendo informação considerada confidencial.	Divulgação de segredo.	Art. 153, Cód. Penal	Detenção de 1 a 6 meses ou multa.
Enviar e-mail dizendo que vai matar a pessoa ou causar-lhe algum mal.	Ameaça.	Art. 147, Cód. Penal	Detenção de 1 a 6 meses ou multa.
Enviar e-mail com remetente falso ou fazer cadastro em loja virtual com nome de terceiros.	Falsa identidade.	Art. 307, Cód. Penal	Detenção de 3 meses a 1 ano ou multa, se o fato não constituir elemento de crime mais grave.
Falar em chat ou comunidade que alguém cometeu algum crime (por exemplo: "fulano é um ladrão").	Calúnia.	Art. 138, Cód. Penal	Detenção de 6 meses a 2 anos e multa.
Efetuar transferência financeira através de internet banking com dados bancários de terceiros.	Furto.	Art. 155, Cód. Penal	Reclusão de 1 a 4 anos e multa.
Funcionário público acessar a rede corporativa e alterar informações sem autorização.	Modificação ou alteração não autorizada de sistemas de informação.	Art. 313-B, Cód. Penal	Detenção de 3 meses a 2 anos e multa.

Direito digital e necessidades atuais

Exemplos:

- Privacidade x monitoramento.
- Segurança da informação x usuário.
- Responsabilidade por atividades realizadas.
- Limites de responsabilidade em ambientes externos.
- Guarda da prova.

Lei de Acesso a Informação

- Lei de acesso a informações públicas, Lei nº 12.527, de 18 de novembro de 2011.
- Trata dos procedimentos a serem observados para o cumprimento do direito constitucional da garantia de acesso às informações.
- Princípio: as informações referentes à atividade do Estado, em qualquer nível, são públicas, salvo exceções expressas na legislação.
- Política de Classificação da Informação.

Verificação da conformidade com requisitos legais

- Legislação vigente.
- Propriedade intelectual.
- Proteção de registros organizacionais.
- Proteção de dados e privacidade de informações pessoais.
- Prevenção do mau uso de recursos de processamento das informações.
- Controles de criptografia.

Legislação vigente

Recomenda-se definir, documentar e manter:

- Requisitos estatutários.
- Requisitos regulamentares.
- Requisitos contratuais.
- Definir e documentar controles específicos e responsabilidades individuais.

Propriedade intelectual

Aplica-se ao uso de:

- Material com direitos autorais.
- Software proprietário.

Recomenda-se implantar procedimentos para garantir a conformidade com os requisitos legais, regulamentares e contratuais.

Cuidados com a propriedade intelectual

- Divulgar política de conformidade (definição do termo “Uso Legal”) com os direitos de propriedade intelectual.
- Adquirir software de boa reputação.
- Conscientizar os envolvidos nos termos das políticas de conformidade.
- Garantir que os ativos possuam requisitos para proteção da propriedade intelectual e manter seus registros.
- Manter provas e evidências da propriedade.
- Controlar o número de licenças em uso.

Verificação da conformidade com políticas e normas de segurança da informação

- Normas de segurança no Brasil.
- Evolução das normas.
- Conformidade com políticas e normas.
- Trabalhando as não-conformidades.
- Conformidade técnica.

Normas de segurança no Brasil

- Em 2001, a ABNT homologou a NBR ISO/IEC 17799:
  - Versão brasileira da BS ISO/IEC 17799.
- Em agosto de 2005, foi liberada a segunda versão da NBR ISO/IEC 17799.
- Em julho de 2007 é atualizada para NBR ISO/IEC 27002.

Roteiro de Atividades 10

Atividade 10.1 – Entendendo a legislação

1. Na sociedade digital moderna, é possível equilibrar segurança, privacidade e funcionalidade ao mesmo tempo? Explique seu ponto de vista.

Atividade 10.2 – Realizando a conformidade

1. Cite e explique pelo menos dois cuidados com a propriedade intelectual citados nas normas ABNT NBR ISO/IEC 27001 e 27002.

2. Quais cuidados devem ser realizados para proteção de registros organizacionais?

3. Quais cuidados sua organização deve ter durante a realização de uma auditoria?

Atividade 10.3 – Executando a conformidade na sua organização

1. Como integrante do comitê de segurança da informação, você resolveu apresentar um plano de verificação da conformidade para sua organização. Considerando a atual estrutura e objetivos da sua instituição, quais serão as legislações que a sua instituição deverá seguir?

2. Como você vai estruturar um processo para que a sua instituição fique em conformidade com as legislações específicas de segurança da informação? Quais deverão ser os objetivos deste trabalho?