GESTÃO DE SEGURANÇA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO SEGUNDO A NBR ISO/IEC 27002 (ANTIGA ISO 17799)

Olá!

Nesta aula, você irá:

Compreender a norma NBR ISO/IEC 27002

1. Conhecer os Conceitos de Segurança da Informação.

2. Normas de Segurança da Informação.

3. Gestão de Riscos segundo a NBR 27001.

4. Política de segurança.

5. Segurança Organizacional.

6. Classificação e controle dos ativos.

7. Segurança em pessoas.

8. Segurança física e do ambiente.

9. Gerenciamento das operações e comunicações.

10. Controle de Acesso.

11. Desenvolvimento e Manutenção de Sistemas.

12. Gestão de incidentes de segurança da informação.

13. Gestão da Continuidade do Negócio.

14. Conformidade.

Você sabe o que é a ISO?

ISO é uma instituição cujo objetivo é propor e monitorar normas que representem e traduzam o consenso de diferentes países para a normalização de procedimentos, medidas e materiais em todos os domínios da atividade produtiva.

Saiba mais

Clique aqui para saber mais sobre a ISO.

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/07GSI_doc01.pdf

Como o Brasil participa da ISO?

Através da ABNT - Associação Brasileira de Normas Técnicas, que é uma sociedade privada sem fins lucrativos. a ABNT (Associação Brasileira de Normas Técnicas), foi fundada em 1940 para fornecer a base necessária ao desenvolvimento tecnológico brasileiro e é o órgão responsável pela normalização técnica no país.

Existem vários grupos participantes da ABNT sobre os mais variados temas. No caso da informática o grupo responsável pela discussão das normas é o:

O CB-21 (Computadores e Processamento de Dados) Este grupo tem como objetivo a normalização no campo de computadores e processamento de dados compreendendo automação bancária, comercial, industrial e do controle de acesso por bilhetes codificados; automação e informática na geração, transmissão e distribuição de dados; segurança em instalações de informática; técnicas criptográficas; gerenciamento em OSI; protocolo de serviços de níveis interiores e cabos e conectores para redes locais, no que concerne a terminologia, requisitos, métodos de ensaio e generalidades.

Aula 7: Segurança da Informação segundo a NBR ISO/IEC 27002

ISO/IEC 27000: Termos e Vocabulário

Esta norma apresenta a descrição, vocabulário e correspondência entre a família de normas que tratam de um Sistema de Gestão de Segurança da Informação (SGSI), proporcionando os fundamentos sobre os quais toda a família está baseada e se integra.

ISO/IEC 27001

Esta norma define os requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SCSI). Especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SCSI documentado dentro do contexto dos riscos de negócio globais da organização, permitindo

que uma empresa construa de forma muito rápida uma política de segurança baseada em controles de segurança eficientes.

ISO/IEC 27002

Esta norma estabelece um referencial para as organizações desenvolverem, implementarem avaliarem a gestão da segurança da informação. Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Ela aborda 11 tópicos:

- Política de Segurança da Informação;
- Organizando a Segurança da Informação;
- Gestão de Ativos;
- Segurança em Recursos Humanos;
- Segurança Física e do Ambiente;
- Gestão das Operações e Comunicações;
- Controle de Acesso;
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- Gestão de Incidentes de Segurança da Informação;
- Gestão da Continuidade do Negócio;
- Conformidade;

ISO/IEC 27003 (Sistema de Gestão de Segurança da Informação: Guia de Implementação)

Esta norma fornece orientação para um sistema de gestão de segurança da informação com objetivos mais amplos que a norma 150 27001, especificamente no que tange à melhoria do desempenho global de uma organização e sua eficiência, assim como sua eficácia.

ISO/IEC 27004

Esta norma define métricas e medições para avaliar a eficácia de um SGSI. Fornece orientações para elaboração, tabulação e acompanhamento de indicadores do sistema de gestão de segurança da informação, visando o acompanhamento dos objetivos de segurança previstos para o sistema de gestão por meio da medição da eficácia dos controles de segurança implementados e permitindo aos gestores avaliar se os controles alcançam de forma satisfatória os objetivos de controle planejados.

ISO/IEC 27005: Gestão de Risco

Fornece diretrizes para o processo de gestão de riscos de segurança da informação. Contém a descrição do processo de gestão de riscos de segurança da informação e das suas atividades.

ISO/IEC 27006:

Guia para o processo de acreditação de entidades certificadoras.

ISO/IEC 27007: Orientações para Gestão de Auditoria de Sistemas de Segurança da Informação.

Esta norma é baseada na norma 150 91011, que apresenta diretrizes de auditoria para os sistemas de gestão de qualidade e/ou ambiental, deve orientar as auditorias de conformidade com a norma ISO 27001.

ISO/IEC 27008: Sistema de Gestão de Segurança da Inforamção - Técnicas de Segurança e Orientações para Auditores de Segurança da Inforamção

Esta norma será um complemento da 150 27007 e deve orientar os Auditores de Sistema de Segurança da Informação a realizar as auditorias dos controles em conformidade com a norma ISO 27001.

Saiba mais

Que entre as organizações que produzem padrões internacionais estão a: IEC (International Electrotechnical Commision) e a ISO.

Segundo a NBR ISO/IEC27002, é essencial que a organização identifique os requisitos de segurança da informação, através de três fontes principais:

Requisitos de Negócio

Uma outra fonte é o conjunto de princípios, objetivos e os requisistos de negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Análise de Risco

A partir da análise/avaliação de riscos levando-se em conta os objetivos e estratégias globais da organização são identificadas as ameaças aos ativos e as vulnerabilidades. É realizada ainda uma estimativa de ocorrência das ameaças e do impacto potencial ao negócio.

Requisitos Legais

Legislação vigente, estatutos, regulamentação e cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço tem que atender.

Analisando/avaliando os riscos de segurança da informação

Segundo a norma NBR ISO/IEC 27002 os riscos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os resultados desta análise ajudarão a direcionar e a determinar as ações gerenciais apropriadas, as prioridades para o gerenciamento dos riscos da segurança da informação e a implementação dos controles selecionados para a proteção contra estes riscos. Após a identificação dos requisitos e dos riscos de segurança da informação e as decisões para o tratamento dos riscos tenham sido tomadas, os controles apropriados devem ser selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável.

Já a norma NBR ISO/IEC 27001 orienta como um organização deve se relacionar com a gestão de risco ao estabelecer seu Sistema de Gestão de Segurança da Informação SGSI. Após definição da política de segurança a organização deve adotar uma abordagem para análise/avaliação de riscos da organização:

A organização deve identificar uma metodologia de análise de risco que seja adequada ao seu SGSI e aos requisitos legais, regulamentares e de segurança da informação identificados em seu negócio;

E desenvolver critérios para aceitação de riscos e identificar os níveis aceitáveis de risco.

Saiba mais

Na norma ISO/IEC TR 13335-3- Information tecnology Part3 são discutidos exemplos de metodologia de análise /avaliação de riscos. Uma outra fonte de pesquisa é a NBR ISO/IEC 31000- Gestão de Risco- princípios e Diretrizes.

Gestão de risco segundo a norma NBR ISO/IEC 27001

- **1**

  A organização deve identificar os riscos, nesta fase deverão ser identificados:

  - Os ativos e seus proprietários dentro do escopo do SGSI;
  - As ameaças e vulnerabilidade destes ativos
  - Os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

-

2

Após a fase de identificação deverão ser analisados e avaliados os riscos levantados. Assim será possível:

- Avaliar os impactos para o negócio da organização que podem resultar de falhas de segurança;
- Avaliar a probabilidade real da ocorrência de falhas de segurança em relação as ameaças e vulnerabilidades identificadas, o impacto decorrente e os controles atualmente implementados.
- Estimar os níveis de riscos e determinar se são aceitáveis ou requerem algum tipo de tratamento.

- **3**

Na próxima etapa a organização deverá identificar e avaliar as opções para tratamento dos riscos que incluem

- Aplicar os controles apropriados;
- Aceitar os riscos desde que satisfaçam as políticas da organização e aos critérios de aceitação do risco;
- Evitar os riscos;
- Transferir os riscos associados ao negócio a outras partes. (Fazer um seguro por exemplo);

- **4**

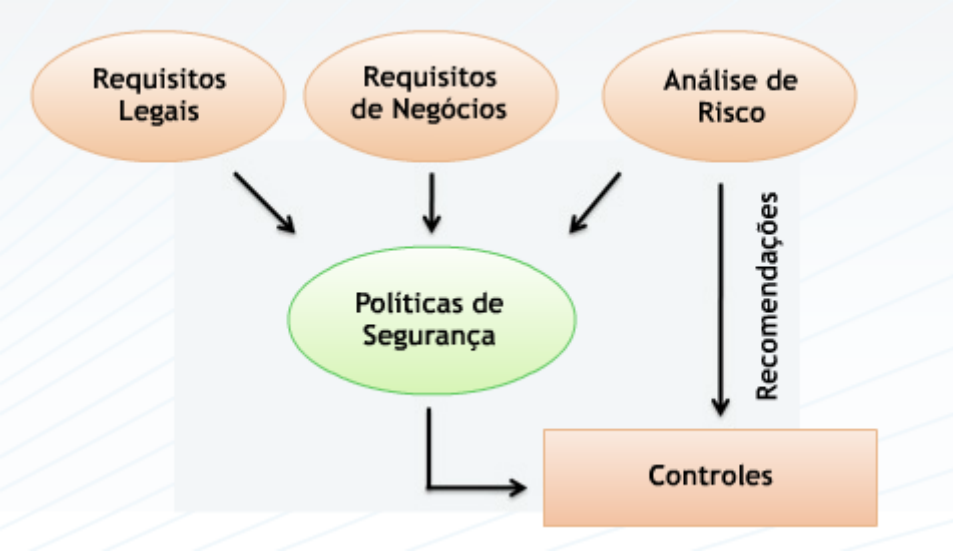
E finalmente selecionar os objetivos de controles e controles para o tratamento dos riscos:

- Os objetivos de controles e controles devem atender aos requisitos identificados pela análise /avaliação de riscos e pelo processo de tratamento de riscos;
- A seleção deve considerar os critérios para a aceitação de riscos com também os requisitos legais, regulamentares e contratuais.

Política de segurança

A norma NBR ISO/IEC 27002 provê uma orientação de como a organização deve proceder para estabelecer a política de segurança da informação:

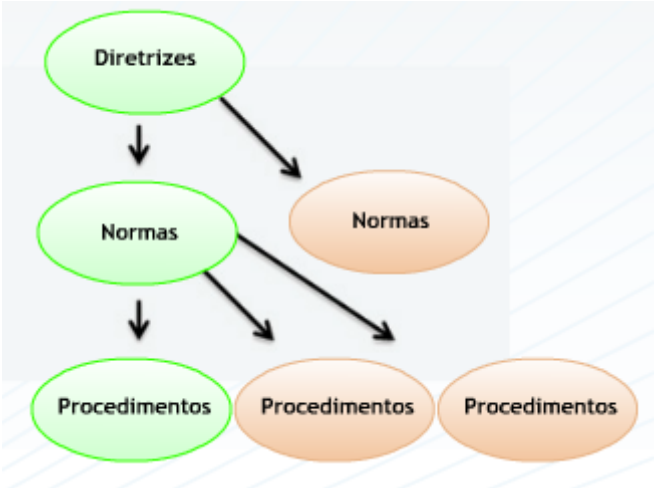
A direção da organização deve estabelecer a orientação da política alinhada com os objetivos do negócio; A direção deve demonstrar seu apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.



Por que a política de segurança é importante?

Serve como linha-mestra para todas as atividades de Segurança da Informação desempenhadas em uma organização pois descreve quais são os objetivos que todas as atividades ligadas à Segurança da Informação devem trabalhar para atingir. Demonstra também o comprometimento da alta direção.

Segundo a NBR ISO/IEC 27002 a política de segurança pode ser parte de um documento da politica geral. Normalmente o documento de política geral é dividido em vários documentos, que são agrupados e estruturados em virtude do nivel de detalhes requeridos, facilitando o desenvolvimento e a manutenção dos documentos e normalmente são dividido em:



As diretrizes são as regras de alto nível que representam os princípios básicos que a organização resolveu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Servem como base para a criação das normas e procedimentos.

As normas especificam no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes.

Os procedimentos detalham no plano operacional, as configurações de um determinado produto ou funcionalidade que devem ser feitas para implementar os controles e tecnologias estabelecidas pela norma.

A NBR ISO/IEC 27002 orienta também que seja realizada a análise crítica dva política de segurança em intervalos regulares ou quando alguma mudança significativa ocorrer de forma a assegurar a eficácia e adequação da política. A análise critica ocorre com a revisão períodica de todo o ciclo de vida da segurança da informação dentro da organização levando em consideração as mudanças que podem ocorrer no ambiente organizacional, nos processos de negócio e nas condições legais da organização.

Organizando a segurança da Informação

A norma NBR ISO/IEC 27002 provê uma orientação de como a organização deve proceder para gerenciar a segurança da informação na organização:

Internamente	• Através do comprometimento da direção; • Através do estabelecimento da coordenação da segurança da informação; • Da atribuição de responsabilidade para a segurança da informação.
Externamente	• Identificação dos riscos relacionados com partes externas • Identificação da segurança antes de conceder aos clientes o acesso aos ativos da organização • Identificação da segurança nos acordos com terceiros

Gestão de Ativos

A norma NBR ISO/IEC 27002 orienta que a organização deve realizar e manter a proteção adequada dos ativos da organização, além de assegurar que a informação receba um nível adequado de proteção.

Mas como implementar?

A organização deverá inventariar todos os ativos e deverá ainda definir um proprietário responsável. Neste inventário deverão ser incluídas todas as informações necessárias que permitam recuperar de um desastre. Estas informações incluem. o tipo do ativo, formato, localização, informações sobre cópia de segurança, informações sobre licenças, a importância do ativo para o negócio assim como a sua classificação de segurança. O proprietário de um ativo pode ser designado para:

- Um processo de negócio;
- Um conjunto de atividade definidas;
- Uma aplicação;
- Um conjunto de dados definido

Saiba mais

Que existem ferramentas automatizadas para realização de inventários dentro de uma organização? Faça uma pesquisa na Internet!

Fique ligado

Segundo a norma NBR ISO/IEC 27002, existem vários tipos de ativo: de informação, de software, físicos, de serviços, pessoas e intangíveis. A norma orienta também que seja realizada a classificação da informação da organização para o devido tratamento das informações que os ativos irão manusear a informação.

Segurança em recursos humanos

A norma NBR ISO/IEC 27002 orienta que a organização assegurar que funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis de forma a reduzir o risco de furto ou roubo, fraude ou mau uso dos recursos. É importante que a responsabilidade pela segurança da informação seja atribuída antes da contratação e que todos os funcionários, fornecedores e terceiros, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação. Conseqüentemente é essencial que a organização documente os papéis e responsabilidades existentes de acordo com a política de segurança da organização.

Vale ressaltar que a preocupação com a segurança deverá ocorrer no momento da: seleção, contratação, encerramento ou mudança da contratação. E a organização deverá ainda preocupar-se com a conscientização, educação e treinamento em segurança da informação, de forma que todos os funcionários e, quando necessário, fornecedores e terceiros recebam treinamentos apropriados em conscientização e atualizações regulares nas políticas e procedimentos organizacionais relevantes para suas funções.

Segurança física e do ambiente

A norma NBR ISO/IEC 27002 orienta que a organização deve prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização. As áreas criticas ou sensíveis deverão ser mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados de forma a não permitir o acesso não autorizado, danos ou interferências.

Deverão ser estabelecidos controles nas entradas físicas das áreas a serem protegidas de forma que somente as pessoas autorizadas tenham acesso. Deverão ser levadas em consideração também a aplicação de níveis de segurança para os escritórios, salas e instalações.

Além da segurança física ao ambiente, a norma prevê a segurança dos equipamentos de forma a impedir perdas, danos, furto ou roubo, ou o comprometimento de ativos e interrupção das atividades da organização. Desta forma é recomendável que os equipamentos sejam protegidos contra as ameaças físicas e do meio ambiente, já estudadas nas aulas anteriormente.

Gerenciamento das operações e comunicações

A norma NBR ISO/IEC 27002 orienta que a organização deve garantir a operação segura e correta dos recursos de processamento da informação. Para isso deverá implementar procedimentos e responsabilidades operacionais assim como a documentação dos procedimentos de operação. Para que as modificações nos recursos de processamento da informação e sistemas sejam controlados, os sistemas operacionais e aplicativos devem estar sujeitos a um rígido controle de gestão de mudanças. É importante também que as funções e áreas de responsabilidades seja segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.

Os recursos dos ambientes de desenvolvimento, teste e produção devem estar separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais, além da implementação de acordos de entrega de serviços terceirizados para garantir que os serviços entregues atendem a todos os requisitos acordados com os terceiros. Para proteger a integridade do software e da informação deverá ser implementado proteção contra códigos maliciosos e códigos móveis não autorizados, além do estabelecimento de procedimentos de rotina para a geração de cópias de segurança assim como a gerencia e o controle adequado das redes de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações, incluindo a informação em trânsito.

Controle de Acesso

A norma NBR ISO/IEC 27002 orienta que a organização deve controlar o acesso à informação, aos recursos de processamento de dados e aos processos de negócios com base nos requisitos de negócio e na segurança da informação levando em consideração as políticas para autorização e disseminação da informação. Desta forma é importante que as regras de controle de acesso e direitos para cada usuário ou grupo de usuário sejam expressas claramente na política de controle de acesso lógico e físico. Para assegurar o acesso de usuário autorizado e prevenir o acesso não autorizado, procedimentos formais devem ser implementados para controlar a distribuição dos direitos de acesso a sistemas de informação e serviços e que cubram todas as fases do ciclo de vida de acesso do usuários. Deve ser realizado o gerenciamento dos privilégios e das senhas do usuário. A

organização deve conscientizar seus usuários sobre suas responsabilidades para garantir o controle efetivo de acesso, principalmente em relação ao uso de senhas e de segurança dos equipamentos de usuários.

Desenvolvimento e Manutenção de Sistemas

A norma NBR ISO/IEC 27002 orienta que a organização deve garantir que segurança é parte integrante de sistemas de informação seja na aquisição, desenvolvimento ou manutenção de Sistemas de Informação. Desta forma os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento ou implementação de sistemas de informação na fase de definição de requisitos de negócios.

Para prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações, devem ser incorporados controles apropriados no projeto de aplicações como forma de assegurar o processamento correto na validação dos dados de entrada, no controle do processamento interno e na validação de dados de saída:

Validação dos dados de entrada

- Entrada duplicada, valores fora de faixa ou caracteres inválidos;
- Dados incompletos ou faltantes;
- Volume de dados excedendo limites superiores ou inferiores;
- Procedimento para tratar erros de validação

Controle de processamento interno

- Garantia de que os riscos de falhas de processamento que levem à perda de integridade sejam minimizados.
- Procedimentos para evitar que programas rodem na ordem errada ou continuem rodando após uma falha de processamento;
- Implementação de técnicas de consistência (hash) para registros e arquivos;
- Proteção contra ataques usando buffer overflow;

Validação dos dados de saída

- Verificações de plausibilidade (Qualidade de ser plausível, de ser admissível. Fonte: /www.dicio.com.b) para testar se os dados de saída são razoáveis;
- Procedimentos para responder aos testes de validação dos dados de saída;
- Criação de um registro de atividades de validação dos dados de saída;

Desenvolvimento e Manutenção de Sistemas

A norma estabelece também o desenvolvimento de uma política para a utilização de controles criptográficos de forma a proteger a confidencialidade, a autenticidade ou a integridade das informações e a implementação de uma política de acesso aos arquivos do sistema e ao código fonte dos sistemas. Um outra abordagem é sobre a segurança no processo de desenvolvimento e de suporte dos aplicativos e informações. Desta forma é conveniente que as organizações controlem os ambientes de projeto e de suporte e que as solicitações de mudanças de software, hardware ou funcionalidade sejam analisadas criticamente para verificar se irão comprometer a segurança do sistema ou do ambiente operacional. A norma recomenda ainda a implementação da gestão de vulnerabilidades técnicas de forma efetiva e sistemática.

Saiba mais

As normas NBR ISO/IEC 10007 trata sobre gestão de configuração, a norma NBR ISO/IEC 12207 trata sobre o processo de ciclo de vida de software e a NBR ISO/IEC 15408 que trata sobre o desenvolvimento seguro de software.

Gestão de incidentes de segurança da informação

A norma NBR ISO/IEC 27002 orienta que a organização deve assegurar que fragilidades e eventos de segurança da informação associados aos sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Desta forma devem ser estabelecidos procedimentos formais de registro e todos os funcionários, fornecedores e terceiros devem estar conscientes sobre estes procedimentos para notificação dos diferentes eventos e fragilidades que possam ter impactos na segurança dos ativos da organização. A norma sugere ainda que um processo de melhoria contínua deve ser implementado às respostas, monitoramento, avaliação e a gestão de incidentes.

Gestão da Continuidade do Negócio

A norma NBR ISO/IEC 27002 orienta que a organização não deve permitir a interrupção das atividades do negócio e deve proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso. Desta forma deverá implementar um processo de continuidade do negócio, aderente à segurança da informação da organização, para minimizar o impacto sobre a organização e recuperar perdas de ativos da informação a um nível aceitável através da combinação de ações de: prevenção e recuperação.

Como implementar?

- Identificação dos processos críticos ;
- Realização de uma análise de impacto dos negócios, através da medição das consequências de desastres, das falhas de segurança, das perda de serviços e disponibilidade dos serviços.
- Realização de análise de risco.

Gestão da Continuidade do Negócio

Em função dos resultados da análise de risco, um plano estratégico deverá ser desenvolvido para determinar a bordagem a ser adotada para a continuidade dos negócios. E uma vez validado pela direção, deverão ser desenvolvidos e implementados os planos de manutenção e recuperação das operações. Etapas da implementação:

- Identificação das responsabilidades e procedimentos de continuidade do negócio;
- Identificação da perda aceitável de informação e serviço;

- Implementação dos procedimentos para a restauração e recuperação das operações do negócio e da disponibilidade da informação nos prazos necessários;
- Documentação dos processo e procedimentos acordados;
- Treinamento do corpo funcional nos procedimentos, processos definidos, incluindo o gerenciamento de crise;
- Teste e atualização dos planos.

É necessário também que seja mantida uma estrutura básica de planejamento para a continuidade de negócios de forma a assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança e identificar prioridades para testes e manutenção.

Conformidade

A norma NBR ISO/IEC 27002 orienta que a organização deve evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

É importante a identificação da legislação aplicável, os direitos de propriedade intelectual, a proteção dos registros organizacionais e o uso de produtos de software proprietários, assim como a conformidade com as políticas e normas de segurança da informação.

O que vem na próxima aula

Gestão de Segurança da Informação Segundo a NBR ISO/IEC 27001

•Assunto 1: Objetivo

•Assunto 2: Abordagem de processo de gestão do SGSI

•Assunto 3: Aplicação da norma

•Assunto 4: Sistema de gestão de segurança da informação (SGSI)

•Assunto 5: Responsabilidades da direção

•Assunto 6: Auditorias internas do SGSI

•Assunto 7: Análise crítica do SGSI pela direção

•Assunto 8: Melhoria do SGSI

CONCLUSÃO

Nesta aula, você:

- Compreendeu a importância da utilização padrões.
- Conheceu as família ISO/IEC 27000.
- Estudou os principais itens da norma ISO/IEC 27001.