Escola Superior de Redes RNP

Gestão da **Segurança da Informação**

NBR 27001 e NBR 27002

Flávia Estélia Silva Coelho
Luiz Geraldo Segadas de Araújo
Edson Kowask Bezerra

A RNP – Rede Nacional de Ensino e Pesquisa – é qualificada como uma Organização Social (OS), sendo ligada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e responsável pelo Programa Interministerial RNP, que conta com a participação dos ministérios da Educação (MEC), da Saúde (MS) e da Cultura (MinC). Pioneira no acesso à Internet no Brasil, a RNP planeja e mantém a rede Ipê, a rede óptica nacional acadêmica de alto desempenho. Com Pontos de Presença nas 27 unidades da federação, a rede tem mais de 800 instituições conectadas. São aproximadamente 3,5 milhões de usuários usufruindo de uma infraestrutura de redes avançadas para comunicação, computação e experimentação, que contribui para a integração entre o sistema de Ciência e Tecnologia, Educação Superior, Saúde e Cultura.

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

Gestão da **Segurança da Informação**

NBR 27001 e NBR 27002

Flávia Estélia Silva Coelho
Luiz Geraldo Segadas de Araújo
Edson Kowask Bezerra

Gestão da **Segurança da Informação**

NBR 27001 e NBR 27002

Flávia Estélia Silva Coelho
Luiz Geraldo Segadas de Araújo
Edson Kowask Bezerra

Rio de Janeiro
Escola Superior de Redes
2014

Rua Lauro Müller, 116 sala 1103
22290-906 Rio de Janeiro, RJ

Diretor Geral
Nelson Simões

Diretor de Serviços e Soluções
José Luiz Ribeiro Filho

Escola Superior de Redes

Coordenação
Luiz Coelho

Edição
Pedro Sangirardi

Revisão
Lincoln da Mata

Coordenação Acadêmica de Segurança e Governança de TI
Edson Kowask Bezerra

Equipe ESR (em ordem alfabética)
Adriana Pierro, Celia Maciel, Cristiane Oliveira, Derlinéa Miranda, Elimária Barbosa, Lourdes Soncin, Luciana Batista, Luiz Carlos Lobato, Renato Duarte e Yve Marcial.

Capa, projeto visual e diagramação
Tecnodesign

Versão
2.0.0

Distribuição
Escola Superior de Redes
Rua Lauro Müller, 116 – sala 1103
22290-906 Rio de Janeiro, RJ
http://esr.rnp.br
info@esr.rnp.br

Dados Internacionais de Catalogação na Publicação (CIP)

C622g Coelho, Flavia Estélia Silva
Gestão da segurança da informação: NBR 27001 e NBR 27002 / Flavia Estélia Silva Coelho, Luiz Geraldo Segadas de Araújo, Edson Kowask Bezerra. – Rio de Janeiro: RNP/ESR, 2014.

Bibliografia: p. 197-198.
ISBN 978-85-63630-12-4

1. Tecnologia da informação - Técnicas de segurança.
2. Sistemas de gestão de segurança da informação - Requisitos. 3. Tecnologia da informação - Código de prática para a gestão de segurança da informação. I. Araújo, Luiz Geraldo Segadas de. II. Bezerra, Edson Kowask. III. Título.

CDD 005.8

Sumário

Escola Superior de Redes

A Escola Superior de Redes (ESR) é a unidade da Rede Nacional de Ensino e Pesquisa (RNP) responsável pela disseminação do conhecimento em Tecnologias da Informação e Comunicação (TIC). A ESR nasce com a proposta de ser a formadora e disseminadora de competências em TIC para o corpo técnico-administrativo das universidades federais, escolas técnicas e unidades federais de pesquisa. Sua missão fundamental é realizar a capacitação técnica do corpo funcional das organizações usuárias da RNP, para o exercício de competências aplicáveis ao uso eficaz e eficiente das TIC.

A ESR oferece dezenas de cursos distribuídos nas áreas temáticas: Administração e Projeto de Redes, Administração de Sistemas, Segurança, Mídias de Suporte à Colaboração Digital e Governança de TI.

A ESR também participa de diversos projetos de interesse público, como a elaboração e execução de planos de capacitação para formação de multiplicadores para projetos educacionais como: formação no uso da conferência web para a Universidade Aberta do Brasil (UAB), formação do suporte técnico de laboratórios do Proinfo e criação de um conjunto de cartilhas sobre redes sem fio para o programa Um Computador por Aluno (UCA).

A metodologia da ESR

A filosofia pedagógica e a metodologia que orientam os cursos da ESR são baseadas na aprendizagem como construção do conhecimento por meio da resolução de problemas típicos da realidade do profissional em formação. Os resultados obtidos nos cursos de natureza teórico-prática são otimizados, pois o instrutor, auxiliado pelo material didático, atua não apenas como expositor de conceitos e informações, mas principalmente como orientador do aluno na execução de atividades contextualizadas nas situações do cotidiano profissional.

A aprendizagem é entendida como a resposta do aluno ao desafio de situações-problema semelhantes às encontradas na prática profissional, que são superadas por meio de análise, síntese, julgamento, pensamento crítico e construção de hipóteses para a resolução do problema, em abordagem orientada ao desenvolvimento de competências.

Dessa forma, o instrutor tem participação ativa e dialógica como orientador do aluno para as atividades em laboratório. Até mesmo a apresentação da teoria no início da sessão de aprendizagem não é considerada uma simples exposição de conceitos e informações. O instrutor busca incentivar a participação dos alunos continuamente.

As sessões de aprendizagem onde se dão a apresentação dos conteúdos e a realização das atividades práticas têm formato presencial e essencialmente prático, utilizando técnicas de estudo dirigido individual, trabalho em equipe e práticas orientadas para o contexto de atuação do futuro especialista que se pretende formar.

As sessões de aprendizagem desenvolvem-se em três etapas, com predominância de tempo para as atividades práticas, conforme descrição a seguir:

Primeira etapa: apresentação da teoria e esclarecimento de dúvidas (de 60 a 90 minutos).
O instrutor apresenta, de maneira sintética, os conceitos teóricos correspondentes ao tema da sessão de aprendizagem, com auxílio de slides em formato PowerPoint. O instrutor levanta questões sobre o conteúdo dos slides em vez de apenas apresentá-los, convidando a turma à reflexão e participação. Isso evita que as apresentações sejam monótonas e que o aluno se coloque em posição de passividade, o que reduziria a aprendizagem.

Segunda etapa: atividades práticas de aprendizagem (de 120 a 150 minutos).
Esta etapa é a essência dos cursos da ESR. A maioria das atividades dos cursos é assíncrona e realizada em duplas de alunos, que acompanham o ritmo do roteiro de atividades proposto no livro de apoio. Instrutor e monitor circulam entre as duplas para solucionar dúvidas e oferecer explicações complementares.

Terceira etapa: discussão das atividades realizadas (30 minutos).
O instrutor comenta cada atividade, apresentando uma das soluções possíveis para resolvê-la, devendo ater-se àquelas que geram maior dificuldade e polêmica. Os alunos são convidados a comentar as soluções encontradas e o instrutor retoma tópicos que tenham gerado dúvidas, estimulando a participação dos alunos. O instrutor sempre estimula os alunos a encontrarem soluções alternativas às sugeridas por ele e pelos colegas e, caso existam, a comentá-las.

Sobre o curso

O propósito do curso é desenvolver competências necessárias para a implementação da gestão da segurança da informação. Durante o curso o participante é apresentado aos conceitos e definições básicas da segurança da informação contido nas normas de segurança ABNT NBR ISO/IEC 27001 e IEC 27002 edição 2013. Com base nelas compreenderá os conceitos de política de segurança e gestão de riscos, conhecerá as boas práticas para a segurança dos recursos humanos e computacionais, segurança física e direito digital. O curso garante ao participante todo o conhecimento necessário para iniciar um processo de implementação da gestão da segurança da informação na sua instituição.

A quem se destina

O curso destina-se aos gestores e profissionais de TIC que necessitam adquirir competências na área de segurança da informação. Também poderão se beneficiar profissionais que desejam aplicar o conhecimento em gestão da segurança da informação em qualquer tipo de organização.

Convenções utilizadas neste livro

As seguintes convenções tipográficas são usadas neste livro:

Itálico
Indica nomes de arquivos e referências bibliográficas relacionadas ao longo do texto.

`Largura constante`

Indica comandos e suas opções, variáveis e atributos, conteúdo de arquivos e resultado da saída de comandos. Comandos que serão digitados pelo usuário são grifados em negrito e possuem o prefixo do ambiente em uso (no Linux é normalmente # ou $, enquanto no Windows é C:\).

Conteúdo de slide
Indica o conteúdo dos slides referentes ao curso apresentados em sala de aula.

Símbolo
Indica referência complementar disponível em site ou página na internet.

Símbolo
Indica um documento como referência complementar.

Símbolo
Indica um vídeo como referência complementar.

Símbolo
Indica um arquivo de áudio como referência complementar.

Símbolo
Indica um aviso ou precaução a ser considerada.

Símbolo
Indica questionamentos que estimulam a reflexão ou apresenta conteúdo de apoio ao entendimento do tema em questão.

Símbolo
Indica notas e informações complementares como dicas, sugestões de leitura adicional ou mesmo uma observação.

Permissões de uso

Exemplo de citação: COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas de. *Gestão da Segurança da Informação – NBR 27001 e 27002*. Rio de Janeiro: Escola Superior de Redes, RNP, 2014.

Comentários e perguntas

Para enviar comentários e perguntas sobre esta publicação:
Escola Superior de Redes RNP
Endereço: Av. Lauro Müller 116 sala 1103 – Botafogo
Rio de Janeiro – RJ – 22290-906
E-mail: info@esr.rnp.br

Sobre o autor

Flávia Estélia Silva Coelho possui Bacharelado em Ciência da Computação e Mestrado em Informática pela Universidade Federal de Campina Grande. Desde 2001, atua em ensino de Graduação e Pós-Graduação Lato Sensu, em projetos de pesquisa e desenvolvimento nas áreas de computação distribuída e segurança da informação. É professora efetiva da Universidade Federal Rural do Semi-Árido (UFERSA), desde 2009, e Java Champion (Oracle), desde 2006.

Luis Geraldo Segadas de Araújo possui especialização em Gestão de Segurança de Informação, Redes de Computadores e Infraestrutura Computacional. Trabalhou para diversas empresas, entre elas a Fundação Petros, tendo atuado também como consultor, com destaque no BNDES e na TBG. Possui experiência em ensino, tendo sido professor na Universidade Estácio de Sá e no Infnet, além de instrutor na RNP/ESR. Possui amplo conhecimento em normas, em especial nas ISO/IEC 27001 e 27002. É Bacharel em Sistemas de Informação pela PUC-RJ, Pós-graduado em Redes de Computadores pela UFRJ e mestre em Administração de Empresas, também na PUC-RJ. Possui as certificações CISSP, CISA e CISM, sendo capacitado em planejamento, elaboração de política de segurança, normas, análise de riscos, diagnóstico e auditoria. Atualmente mora no Canadá.

Edson Kowask Bezerra é profissional da área de segurança da informação e governança há mais de quinze anos, atuando como auditor líder, pesquisador, gerente de projeto e gerente técnico, em inúmeros projetos de gestão de riscos, gestão de segurança da informação, continuidade de negócios, PCI, auditoria e recuperação de desastres em empresas de grande porte do setor de telecomunicações, financeiro, energia, indústria e governo. Com vasta experiência nos temas de segurança e governança, tem atuado também como palestrante nos principais eventos do Brasil e ainda como instrutor de treinamentos focados em segurança e governança. É professor e coordenador de cursos de pós-graduação na área de segurança da informação, gestão integrada, de inovação e tecnologias web. Hoje atua como Coordenador Acadêmico de Segurança e Governança de TI da Escola Superior de Redes.

1

Fundamentos da segurança da informação

objetivos

Explicar as definições mais importantes e preocupações comuns a considerar em termos de segurança da informação nas organizações; Selecionar serviços e controles para a segurança da informação e identificar os fatores críticos de sucesso.

conceitos

Serviços de segurança; Gestão da segurança da informação; Ameaças, vulnerabilidades, ataques e controles.

Por que se preocupar com segurança?

Problemas mais comuns:

- Destruição de informações e outros recursos.
- Modificação ou deturpação de informações.
- Roubo, remoção ou perda da informação ou de outros recursos.
- Revelação de informações.
- Interrupção de serviços.

As organizações cada vez mais reconhecem o valor e as vulnerabilidades de seus ativos.

Exercício de nivelamento 1
Fundamentos de segurança da informação

O que é segurança para você?

O que você entende por segurança da informação?

A segurança da informação é um ponto crítico para a sobrevivência das organizações na era da informação. Vários são os problemas envolvidos, ao passo que a sociedade depende das informações armazenadas nos sistemas computacionais para a tomada de decisão em empresas, órgãos do governo, entre outros contextos organizacionais.

A informação pode existir em diversos formatos: impressa, armazenada eletronicamente, falada, transmitida pelo correio convencional de voz ou eletrônico etc. Seja qual for o formato ou meio de armazenamento ou transmissão, recomenda-se que ela seja protegida adequadamente. Sendo assim, é de responsabilidade da segurança da informação protegê-la de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar riscos e maximizar o retorno dos investimentos.

Felizmente, é crescente a conscientização das organizações frente ao valor e às vulnerabilidades de seus ativos no que diz respeito à segurança. Hoje em dia, a segurança da informação é determinante para assegurar competitividade, lucratividade, atendimento aos requisitos legais e a imagem da organização junto ao mercado, às organizações, tanto no setor público quanto no setor privado. Em tais contextos, a segurança da informação é um componente que viabiliza negócios, tais como e-Gov (governo eletrônico) ou e-commerce (comércio eletrônico).

Definições

- Segurança da informação.
- Incidente de segurança.
- Ativo.
- Ameaça.
- Vulnerabilidade.
- Risco.
- Ataque.
- Impacto.

Segurança da Informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança. Todos esses controles necessitam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados para que assegurem que os objetivos do negócio e a segurança da informação da organização sejam atendidos (item 0.1 da norma ABNT NBR ISO/IEC 27002:2013).

A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.

Em particular, os controles necessitam ser estabelecidos, implementados, monitorados, analisados e continuamente melhorados, com o intuito de atender aos objetivos do negócio e de segurança da organização. A identificação de controles adequados requer um planejamento detalhado. A seguir são detalhados alguns conceitos:

- **Incidente de segurança**: corresponde a qualquer evento adverso relacionado à segurança; por exemplo, ataques de negação de serviços (Denial of Service – DoS), roubo de informações, vazamento e obtenção de acesso não autorizado a informações;
- **Ativo**: qualquer coisa que tenha valor para a organização e para os seus negócios. Alguns exemplos: banco de dados, softwares, equipamentos (computadores e notebooks), servidores, elementos de redes (roteadores, switches, entre outros), pessoas, processos e serviços;

- **Ameaça**: qualquer evento que explore vulnerabilidades. Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **Vulnerabilidade**: qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidades são falhas que permitem o surgimento de deficiências na segurança geral do computador ou da rede. Configurações incorretas no computador ou na segurança também permitem a criação de vulnerabilidades. A partir dessa falha, as ameaças exploram as vulnerabilidades, que, quando concretizadas, resultam em danos para o computador, para a organização ou para os dados pessoais;
- **Risco**: combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a organização. Algo que pode ocorrer e seus efeitos nos objetivos da organização;
- **Ataque**: qualquer ação que comprometa a segurança de uma organização;
- **Impacto**: consequência avaliada de um evento em particular.

Exercício de fixação 1
Definições

Explique o que são ativos.

Como você explicaria na sua organização o termo “vulnerabilidade”?

Modelos de ataque

- Interrupção.
- Interceptação.
- Modificação.
- Fabricação.

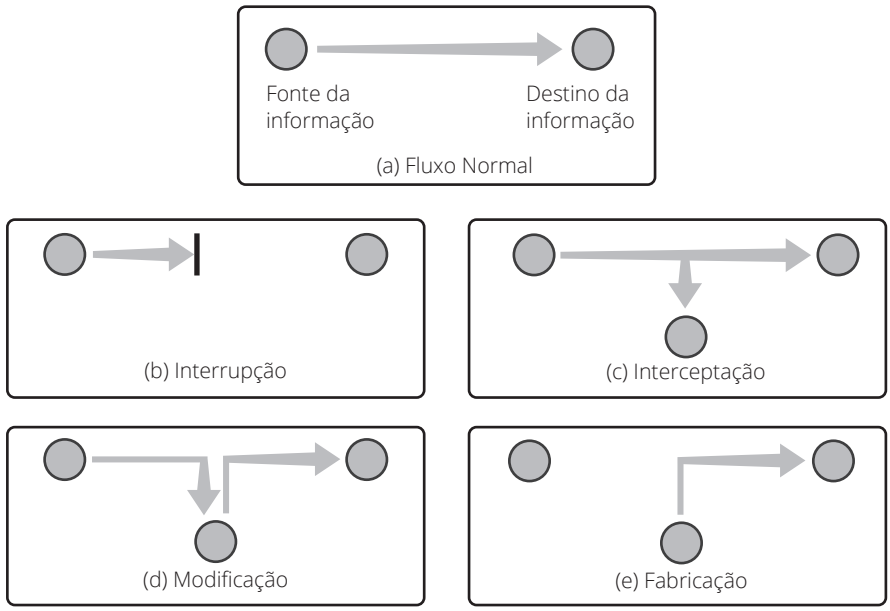


Figura 1.1
Modelos de ataque.

Há quatro modelos de ataque possíveis:

- **Interrupção**: quando um ativo é destruído ou torna-se indisponível (ou inutilizável), caracterizando um ataque contra a disponibilidade. Por exemplo, a destruição de um disco rígido;
- **Interceptação**: quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador), caracterizando um ataque contra a confidencialidade. Por exemplo, cópia não autorizada de arquivos ou programas;
- **Modificação**: quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador) e ainda alterado, caracterizando um ataque contra a integridade. Por exemplo, mudar os valores em um arquivo de dados;
- **Fabricação**: quando uma parte não autorizada (pessoa, programa ou computador) insere objetos falsificados em um ativo, caracterizando um ataque contra a autenticidade. Por exemplo, a adição de registros em um arquivo.

Na figura 1.1, observamos o fluxo normal da informação de uma origem para um destino (a). Na sequência, o esquema apresenta cada um dos modelos de ataques possíveis: uma interrupção (b), interceptação (c), modificação (d) e fabricação (e).

Exercício de fixação 2
Modelos de ataque

Explique o modelo de ataque da interceptação.

Formas de ataque

Ataques passivos:

- Resultam na liberação dos dados.

Ataques ativos:

- Resultam na alteração ou destruição dos dados.

O ataque é um ato deliberado de tentar se desviar dos controles de segurança com o objetivo de explorar as vulnerabilidades. Existem as seguintes formas de ataque:

- **Ataques passivos**: ataques baseados em escutas e monitoramento de transmissões, com o intuito de obter informações que estão sendo transmitidas. A escuta de uma conversa telefônica é um exemplo dessa categoria. Ataques dessa categoria são difíceis de detectar porque não envolvem alterações de dados; todavia, são possíveis de prevenir com a utilização de criptografia;
- **Ataques ativos**: envolvem modificação de dados, criação de objetos falsificados ou negação de serviço, e possuem propriedades opostas às dos ataques passivos. São ataques de difícil prevenção, por causa da necessidade de proteção completa de todas as facilidades de comunicação e processamento, durante o tempo todo. Sendo assim, é possível detectá-los e aplicar uma medida para recuperação de prejuízos causados.

Exercício de fixação 3
Formas de ataque

Explique dentro do ambiente da sua organização como ocorreria um ataque ativo.

Arquitetura de segurança

- Proteção de dados contra modificações não autorizadas.
- Proteger os dados contra perda/roubo/furto.
- Proteção de dados contra a divulgação não autorizada.
- Garantir a identidade do remetente correto dos dados.
- Garantir a identidade correta do destinatário dos dados.

A arquitetura de segurança proposta pelo modelo ISA (interconexão de sistemas abertos), definido na norma ISO 7498-2, estabelece os seguintes objetivos ou requisitos de segurança:

1. Proteção de dados contra modificações não autorizadas;
2. Proteger os dados contra perda/furto/roubo;
3. Proteção de dados contra a divulgação não autorizada;
4. Garantir a identidade do remetente correto dos dados;
5. Garantir a identidade correta do destinatário dos dados.

Serviços de segurança

Objetivos:

- Aumento da segurança.
- Utilização de mecanismos de segurança.

Categorias de serviços de segurança.

- Confidencialidade.
- Autenticidade.
- Integridade.
- Não repúdio.
- Conformidade.
- Controle de acesso.
- Disponibilidade.

Neste tópico, serão tratados os objetivos e categorias de serviços de segurança a serem considerados no contexto da segurança da informação. De acordo com o padrão ISO 7498-2, que compreende os aspectos relacionados à segurança no modelo Open Systems Interconnection (OSI), os serviços de segurança são medidas preventivas escolhidas para combater ameaças identificadas. Os serviços de segurança aumentam a segurança da informação contra ataques fazendo uso de um ou mais mecanismos de segurança. Em muitas literaturas esses serviços também são citados como princípios básicos de segurança.

Os serviços e mecanismos de segurança devem ser aplicados de modo a atender aos requisitos de segurança da organização, levando em consideração o equilíbrio entre as necessidades de segurança e custos respectivos. Em especial, ao identificar e priorizar serviços de segurança, é essencial fazer uma análise dos riscos e impactos prováveis que compreendem toda a organização em questão.

- **Confidencialidade**: compreende a proteção de dados transmitidos contra ataques passivos, isto é, contra acessos não autorizados, envolvendo medidas como controle de acesso e criptografia. A perda da confidencialidade ocorre quando há uma quebra de sigilo de uma determinada informação (exemplo: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários;
- **Autenticidade**: está preocupada em garantir que uma comunicação é autêntica, ou seja, origem e destino podem verificar a identidade da outra parte envolvida na comunicação, com o objetivo de confirmar que a outra parte é realmente quem alega ser. A origem e o destino tipicamente são usuários, dispositivos ou processos;
- **Integridade**: trata da garantia contra ataques ativos por meio de alterações ou remoções não autorizadas. É relevante o uso de um esquema que permita a verificação da integridade dos dados armazenados e em transmissão. A integridade pode ser considerada sob dois aspectos: serviço sem recuperação ou com recuperação. Uma vez que os ataques ativos são considerados no contexto, a detecção, em vez da prevenção, é o que importa; então, se o comprometimento da integridade é detectado, pode-se reportá-lo e o mecanismo de recuperação é imediatamente acionado. A integridade também é um pré-requisito para outros serviços de segurança. Por exemplo, se a integridade de um sistema de controle de acesso a um Sistema Operacional for violada, também será violada a confidencialidade de seus arquivos. A perda de integridade surge no momento em que uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação;
- **Não repúdio**: compreende o serviço que previne uma origem ou destino de negar a transmissão de mensagens, isto é, quando dada mensagem é enviada, o destino pode provar que esta foi realmente enviada por determinada origem, e vice-versa;

- **Conformidade**: dever de cumprir e fazer cumprir regulamentos internos e externos impostos às atividades da organização. Estar em conformidade é estar de acordo, seguindo e fazendo cumprir leis e regulamentos internos e externos;
- **Controle de acesso**: trata de limitar e controlar o acesso lógico/físico aos ativos de uma organização por meio dos processos de identificação, autenticação e autorização, com o objetivo de proteger os recursos contra acessos não autorizados;
- **Disponibilidade**: determina que recursos estejam disponíveis para acesso por entidades autorizadas, sempre que solicitados, representando a proteção contra perdas ou degradações. A perda de disponibilidade acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

Exercício de fixação 4
Serviços de segurança

Explique como sua organização protege a confidencialidade.

Explique o que vem a ser autenticidade e integridade.

Segurança da informação

Visão geral de gestão da segurança da informação:

- Preparando a organização.
- Requisitos de segurança.
- Análise/avaliação de riscos.
- Seleção de controles.
- Itens relevantes.
- Atividades envolvidas.

Neste tópico, são detalhados os aspectos principais relacionados à gestão da segurança da informação, com a apresentação de uma visão geral das preocupações, responsabilidades e atividades envolvidas.

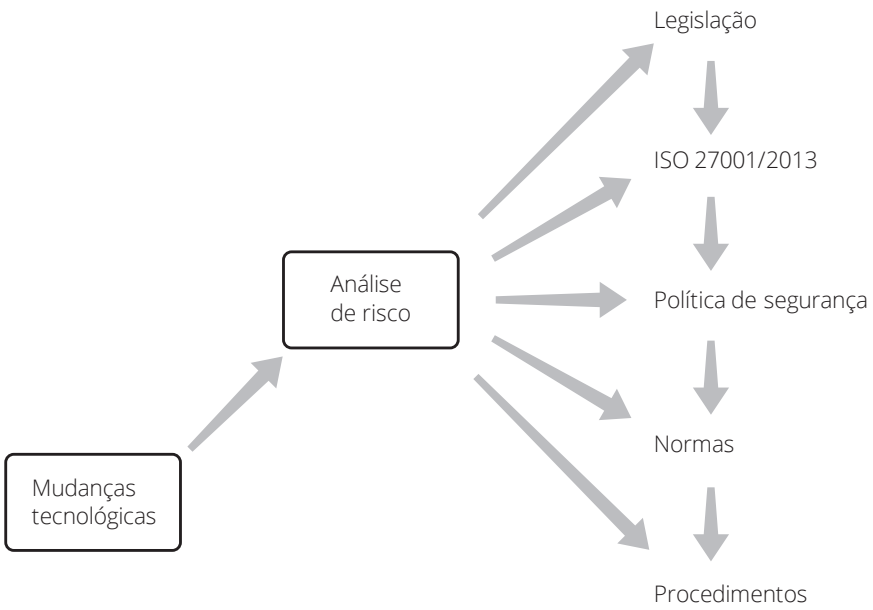


Figura 1.2
Visão geral da segurança da informação.

A figura 1.2 apresenta uma visão geral da segurança da informação. As mudanças tecnológicas são uma constante presença no dia a dia da organização. Essas mudanças podem fazer surgir novas vulnerabilidades e riscos, ou ainda aumentar os já existentes, o que precisa ser acompanhado através de uma análise de riscos dinâmica e atualizada, permitindo o levantamento dos níveis dos riscos e da forma de tratá-los.

Simultaneamente é necessário conhecer a legislação que a organização é obrigada a seguir e a levantar os requisitos de segurança necessários para atendê-la. A partir desses requisitos legais, identificar os controles necessários e aqueles apontados pela análise de risco, com o uso das normas de segurança. A partir dos controles identificados, é necessário gerar as políticas, normas e procedimentos para a implementação dos controles.

Preparando a organização

É preciso ter em mente as respostas aos seguintes questionamentos:

- O que proteger?
- Contra o quê ou quem?
- Qual a importância de cada recurso?
- Qual o grau de proteção desejado?
- Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados?
- Quais as expectativas dos diretores, clientes e usuários em relação à segurança da informação?

Antes de pensar em gestão da segurança da informação em uma organização, é preciso ter em mente as respostas aos seguintes questionamentos:

1. O que proteger? Ativos da organização necessitam de proteção.
2. Contra o quê ou quem? Quais são as ameaças que podem afetar a organização e de que forma e por quem essas ameaças podem ser exploradas.

3. Qual a importância de cada recurso? Como cada recurso de informação participa do **processo de negócio** da organização.

Processo de negócio
Conjunto de ações e atividades que coexistem e interagem entre si de forma lógica e coerente para desenvolver um entregável (produto) que atenda aos requisitos de qualidade e às expectativas do cliente, seja ele interno ou externo.

4. Qual o grau de proteção desejado? Que requisitos de proteção o negócio exige e que nível de proteção é necessário.
5. Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados? Que recursos estão disponíveis para os objetivos de segurança e o que pode ser feito com os recursos existentes.
6. Quais as expectativas dos diretores, clientes e usuários em relação à segurança da informação? O que eles esperam da segurança da informação para o negócio da organização.

Com respostas a essas perguntas, pode-se prosseguir com o processo de estabelecimento da segurança da informação e de sua gestão na organização.

Requisitos de segurança

Há três fontes a considerar:

- Análise/avaliação de riscos da organização.
- Legislação vigente, estatutos, regulamentações e cláusulas contratuais da organização.
- Conjunto de princípios, objetivos e requisitos do negócio.

Há três fontes principais a considerar ao estabelecer os requisitos de segurança da informação de uma organização:

- **Análise/avaliação de riscos**: considera os objetivos e estratégias de negócio da organização, resultando na identificação de vulnerabilidades e ameaças aos ativos. Nesse contexto, leva-se em conta a probabilidade de ocorrência de ameaças e o impacto para o negócio.
- **Legislação vigente**: estatutos, regulamentação e cláusulas contratuais a que devem atender a organização, seus parceiros, terceirizados e fornecedores.
- **Conjunto de princípios**: objetivos e requisitos de negócio para o processamento de dados que a organização deve definir para dar suporte às suas operações.

Mais informações podem ser consultadas na norma ABNT ISO/IEC 27002:2013 no item 0.2.

Análise/avaliação de riscos

- Gastos com controles precisam ser balanceados de acordo com os dados potenciais.
- Resultados direcionam e determinam ações gerenciais.
- Tarefa periódica, para contemplar mudanças.

Mais informações podem ser obtidas na norma ABNT NBR ISO/IEC 27005:2013.

Na análise/avaliação de riscos, os gastos com os controles devem ser balanceados de acordo com o impacto que falhas potenciais de segurança causarão aos negócios. Sendo assim, deve ser efetuada periodicamente, com o intuito de contemplar mudanças na organização.

Os resultados auxiliam no direcionamento e determinação das ações gerenciais e das prioridades para o gerenciamento de riscos da segurança da informação. A avaliação compara o risco estimado com critérios predefinidos para determinar a importância ou valor do risco para a organização.

Seleção de controles

- Controles devem ser implementados para garantir a redução de riscos.
- Dependem das decisões da organização quanto aos riscos.
- Podem ser selecionados a partir de normas preestabelecidas ou de conjunto de controles específicos. Por exemplo, as normas:
  - ABNT NBR ISO/IEC 27002:2013.
  - ABNT NBR ISO/IEC 27001:2013.

Após a identificação de requisitos de segurança, análise/avaliação dos riscos e tomadas de decisão quanto ao tratamento de riscos em uma organização, pode-se, enfim, selecionar e implementar os controles adequados.

Controles são medidas ou um conjunto de medidas adotadas para tratar vulnerabilidades e reduzir o risco de incidentes de segurança da informação. Controle, também conhecido como contramedida, corresponde a qualquer mecanismo útil para gerenciar riscos, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais — que podem ser de natureza administrativa, técnica, de gestão ou legal.

Os controles podem ser selecionados a partir de normas preestabelecidas (por exemplo, as normas ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27001:2013) ou de um conjunto de controles específicos para a organização. Em particular, os controles selecionados devem estar de acordo com a legislação e regulamentação nacionais e internacionais vigentes e relevantes à segurança da informação e ao negócio da organização.

Alguns exemplos de controle:

- Barreiras, portas, cartazes de "proibida a entrada" e catracas;
- Crachás, controle de visitantes e CFTV;
- Senhas, fechaduras e **controles biométricos**;
- Políticas de segurança, termos de responsabilidade e treinamento;
- Antivírus, backup e controle de acesso lógico.

Controles biométricos

Uso da biometria para verificar ou identificar acesso a recursos como computadores, notebooks, smartphones, redes de computadores, aplicações, bases de dados e outros hardwares e softwares que necessitem ter o seu acesso protegido. Biometria é o uso de características físicas ou comportamentais das pessoas como forma de identificá-las unicamente.

Exercício de fixação 5
Seleção de controles

Explique o que são controles.

Controles para a segurança da informação

Controles considerados essenciais, do ponto de vista legal:

- Proteção de dados e privacidade.
- Proteção de registros organizacionais.
- Direitos de propriedade intelectual.

Controle, por definição, é um modo de gerenciar riscos, podendo incluir políticas, procedimentos, diretrizes e práticas que podem ser de natureza administrativa, técnica, legal ou de gestão. Alguns controles podem ser considerados como “primeiros passos” para a segurança da informação nas organizações, tendo como base requisitos legais e/ou melhores práticas para a segurança da informação.

Sob o ponto de vista legal, há os controles considerados essenciais e que dependem da legislação vigente, a saber:

- Proteção de dados e privacidade de informações pessoais;
- Proteção de registros organizacionais;
- Direitos de propriedade intelectual.

Controles considerados como boas práticas:

- Política de segurança da informação.
- Atribuição de responsabilidades.
- Conscientização, educação e treinamento em segurança da informação.
- Processamento correto em aplicações.
- Gestão de vulnerabilidades.
- Gestão da continuidade do negócio.
- Gestão de incidentes de segurança da informação.

Já os controles considerados como boas práticas para a segurança da informação compreendem:

- Documento da política de segurança da informação;
- Atribuição de responsabilidades para a segurança da informação;
- Conscientização, educação e treinamento em segurança da informação;
- Processamento correto nas aplicações;
- Gestão das vulnerabilidades técnicas;
- Gestão da continuidade do negócio;
- Gestão de incidentes de segurança da informação.

Vale ressaltar que selecionar ou não determinado controle deve ser uma ação baseada nos riscos específicos da organização. Sendo assim, considere os controles apontados como ponto de partida, uma vez que estes não substituem a seleção de controles baseada na análise/avaliação de riscos.

É notória, ainda, a conscientização de que uma política de segurança da informação não deve ser definida de modo genérico. As organizações devem ser analisadas caso a caso, de forma a identificar suas necessidades de segurança para que, assim, seja desenvolvida e implantada uma política adequada. Em adição, a política deve atribuir direitos e responsabilidades às entidades que lidam diretamente com informações e recursos computacionais das organizações. Sendo assim, qualquer evento que resulte em descumprimento da política é considerado incidente de segurança.

Outra questão a ser considerada é a gestão da continuidade do negócio, a qual preocupa-se com planos de contingência e de continuidade, com destaques para o planejamento para garantir a recuperação após desastres.

Exercício de fixação 6
Controles para a segurança da informação

Quais são os controles considerados essenciais sob o ponto de vista legal?

Na sua organização, quais controles aplicados são considerados como melhores práticas?

Itens relevantes para a segurança da informação

- Política de segurança da informação.
- Segurança organizacional.
- Gestão de ativos.
- Segurança em Recursos Humanos.
- Segurança física e de ambiente.
- Gerenciamento de operações e comunicações.
- Controle de acesso.
- Aquisição, desenvolvimento e manutenção de SI.
- Gestão de incidentes de segurança.
- Gestão da continuidade do negócio.

A gestão da segurança da informação incentiva a adoção de políticas, procedimentos, guias e demais elementos relevantes, cujo escopo deve compreender o gerenciamento de riscos baseado em análises de custo/benefício para a organização.

Nesse contexto, para a gestão da segurança da informação, os itens listados a seguir são relevantes:

- Política de segurança da informação;
- Segurança organizacional;
- Gestão de ativos;
- Segurança em Recursos Humanos;
- Segurança física e do ambiente;
- Gestão das operações e comunicações;
- Controle de acesso;
- Gestão de incidentes de segurança da informação;
- Gestão da continuidade do negócio.

Todos os itens são tratados em detalhes na norma ABNT NBR ISO/IEC 27002:2013 e serão explicados na sequência deste curso.

Atividades envolvidas

- Gerência de segurança dos sistemas.
- Gerência dos serviços de segurança.
- Gerência dos mecanismos de segurança.
- Gerência da auditoria de segurança.

Atividades adicionais consideradas no escopo da gestão da segurança da informação:

- Gestão da segurança dos sistemas, que engloba todos os aspectos de segurança dos sistemas de uma organização, tais como administração da política de segurança, procedimentos de recuperação após desastres, entre outros. É de responsabilidade desta gerência a constante atualização com respeito a problemas, riscos e soluções de segurança mais recentes;
- Gerência de serviços de segurança, incluindo a seleção dos mecanismos de segurança mais adequados para atendê-los;
- Gerência dos mecanismos de segurança disponíveis para atender aos requisitos de segurança da organização;
- Gerência da auditoria de segurança, revisando e verificando registros e eventos de segurança, com o objetivo de avaliar a adequação dos controles do sistema, sua aderência à política de segurança, e de recomendar mudanças adequadas ou necessárias aos controles empregados na organização.

Fatores críticos para o sucesso da segurança da informação

Fatores críticos para o sucesso:

- Política de segurança da informação.
- Abordagem e estrutura para implementação, manutenção, monitoramento e melhorias da segurança da informação.
- Comprometimento dos níveis gerenciais.
- Entendimento dos requisitos de segurança da informação, da análise, avaliação e gestão de riscos.
- Divulgação eficiente.

A seguir, são apresentados alguns fatores considerados críticos para o sucesso da segurança da informação nas organizações:

- A política de segurança da informação, objetivos e práticas devem refletir os objetivos de negócio da organização;
- A abordagem e a estrutura adotadas para a implementação, manutenção, monitoramento e melhoria da segurança da informação devem ser compatíveis com a cultura da organização;
- Todos os níveis gerenciais da organização devem estar comprometidos e apoiando a segurança da informação;
- Os requisitos de segurança da informação, a análise, avaliação e **gestão de riscos** devem ser bem entendidos (e em detalhes);
- A segurança da informação deve ser divulgada, de modo eficiente, a todas as entidades da organização (presidentes, diretores, gerentes, funcionários, contratados etc.).

Gestão de riscos

Envolve atividades para direcionar e controlar uma organização em termos de riscos. Sendo assim, compreende análise, avaliação, tratamento e aceitação de riscos.

- Distribuição e comunicação de diretrizes, políticas e normas para todas as partes envolvidas.
- Provisão de recursos financeiros para a gestão da segurança da informação.
- Provisão da conscientização, treinamento e educação adequados.
- Estabelecimento de um processo eficiente de gestão de incidentes de segurança.
- Implementação de um sistema de medição da gestão da segurança da informação.

- Todos os itens da política de segurança devem ser distribuídos e comunicados para as entidades da organização.
- Recursos financeiros devem ser providos para a gestão da segurança da informação.
- Meios de conscientização, treinamento e educação adequados devem ser providos.
- Deve-se estabelecer um processo eficiente para a gestão de incidentes de segurança da informação.
- É preciso implantar um mecanismo para medir e avaliar a efetividade da gestão da segurança da informação, com subsequentes sugestões de melhorias.

Roteiro de Atividades 1

Atividade 1.1 – Identificando ataques

Para cada situação a seguir, indique o modelo de ataque aplicável. Justifique sua resposta:

Situação	Modelo de ataque	Justificativa
Adição de um registro falsificado em um banco de dados.		
Desabilitar um sistema de arquivos.		
Modificação de dados trafegando na rede.		
Inutilização física de um componente de hardware.		
Captura de dados em rede, através de escutas.		
Alteração de um programa para que execute de modo diferente.		

Atividade 1.2 – Identificando vulnerabilidades

Para cada uma das situações a seguir, cite pelo menos uma vulnerabilidade possível de ser explorada para concretizar uma ameaça à segurança da informação de uma organização. Justifique as suas respostas:

1. Pessoal de serviço diário de mensageiro realizando entrega e coleta de mensagens.

2. Ex-funcionários que deixaram a empresa porque foram dispensados.

3. Funcionário viajando a serviço da organização e acessando a rede remotamente.

4. Utilização de notebook pessoal sem cadastro na lista de ativos.

5. Computador de trabalho logado, sem o usuário nas proximidades.

Atividade 1.3 – Identificando a forma de ataque

Identifique a forma de ataque aplicável a cada situação a seguir. Justifique sua resposta:

1. Captura e acesso a um arquivo transferido de um cliente a um servidor via rede.

2. Alteração de parte de uma mensagem legítima.

3. Análise de tráfego de uma rede, utilizando um sniffer.

4. Interrupção de uma rede, por causa de uma sobrecarga de tráfego que degradou a sua performance.

5. Utilização de login e senha de outro usuário.

Atividade 1.4 – Associando categorias de serviços de segurança

Para cada contexto apresentado a seguir, indique o(s) serviço(s) diretamente associado(s):

1. Manutenção de informações secretas, realizada por meio de códigos para a transmissão em rede.

2. Duplicação de servidores de missão-crítica.

3. Não abrir arquivos ou executar programas anexados em e-mails sem antes verificá-los com um antivírus.

4. Usuários devem declarar por que são necessárias alterações em seus privilégios na organização e a relação do pedido com as atividades por ele desempenhadas.

5. É vedado aos usuários o direito de modificar, remover ou copiar arquivos que pertençam a outro usuário, sem a sua permissão expressa.

Atividade 1.5 – Estudo de caso: sua organização

Considerando sua organização atualmente, faça uma rápida análise da situação da segurança da informação e responda:

1. Quais são os controles do ponto de vista legal e de boas práticas que sua organização necessita? Justifique.

2. Quais são os fatores críticos de sucesso da segurança da informação na sua organização?

2

Código de prática

objetivos

Conhecer a norma ABNT NBR ISO/IEC 27002:2013 e selecionar, relacionar e combinar seus controles.

conceitos

Estrutura e seções da norma ABNT NBR ISO/IEC 27002:2013 e seus objetivos.

Estrutura da norma

A norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação), foi preparada para servir como um guia prático para o desenvolvimento e a implementação de procedimentos e controles de segurança da informação em uma organização.

Exercício de nivelamento 1
Código de prática

O que você entende por código de prática?

Estrutura da norma

Apresentação da norma ABNT NBR ISO/IEC 27002:2013:

- Possui 14 seções.
- Possui 35 objetivos de controle.
- A versão atual possui 114 controles.

Estruturada para fornecer um código de boas práticas para gestão da segurança, a norma é organizada em capítulos de 0 a 18. Os capítulos de 0 a 4 apresentam os temas de introdução (0), Escopo (1), Referência normativa (2), Termos e definições (3) e Estrutura desta norma (4).

A partir do capítulo 5, a norma passa a chamar cada capítulo de seção. Assim, existem catorze seções específicas apresentando os códigos de práticas da gestão da segurança.

Cada seção define um ou mais objetivos de controle. As catorze seções formam o total de 35 objetivos de controle. A seção 4 da norma apresenta sua estrutura.

Existem 114 controles e eles são os elementos que definem o que a norma 27002 considera como importante para um processo de segurança da informação. Os controles identificados por números (xx.xx.xx) são estruturados através de:

> Os controles da norma são apresentados como boas praticas para que a organização adote uma postura preventiva e pró ativa diante das suas necessidades e requisitos de segurança da informação.

- **Controle**: descrição e definição do controle;
- **Diretrizes para a implementação**: informações auxiliares mais detalhadas na implementação do controle;
- **Informações adicionais**: informações complementares.

Todo o trabalho deste capítulo será desenvolvido com o manuseio e leitura dos tópicos apresentados na norma NBR ISO/IEC 27002:2013.

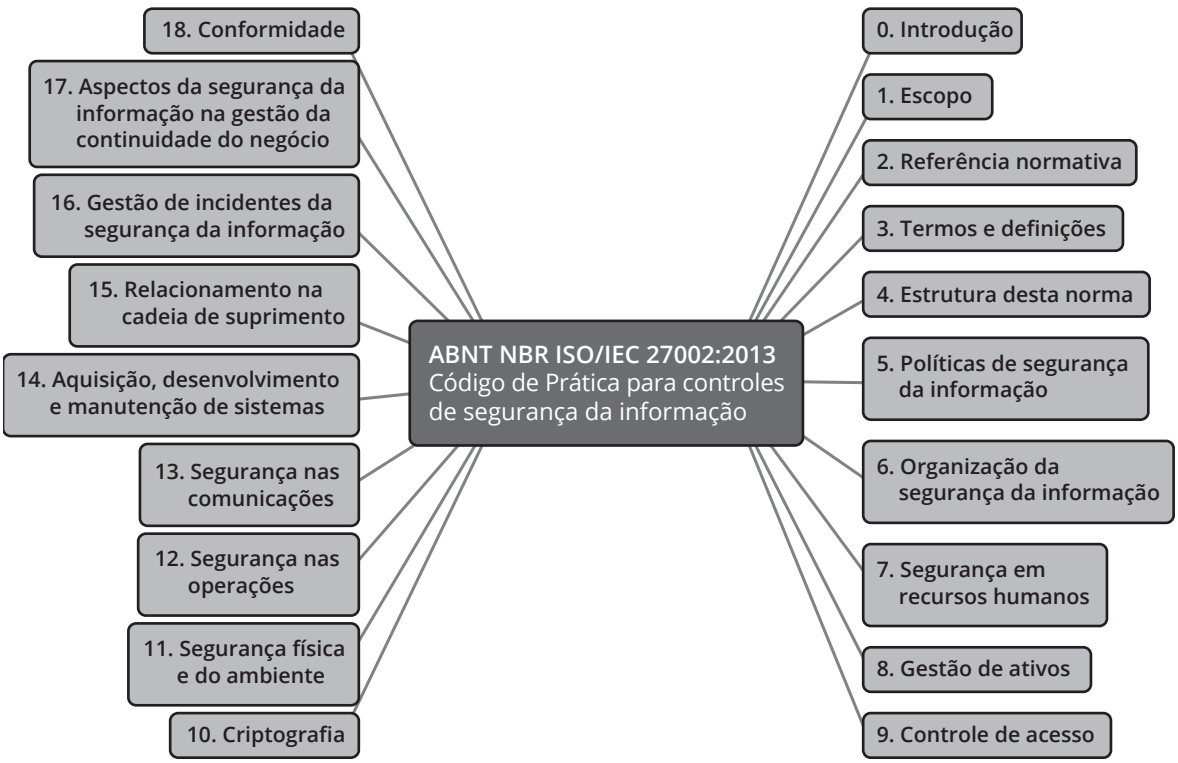


Figura 2.1 Sequência estrutural da norma.

No sentido horário, observa-se a sequência estrutural da norma destacando-se as catorze seções de controles de segurança da informação (seções de 5 a 18).

Seção 5 – Políticas de segurança da informação

5.1. Política de segurança da informação

- Objetivo:
  - Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

A seção 5 da norma trata da política de segurança da informação e seus requisitos. O objetivo da categoria de controle é fornecer orientação e apoio da direção para a segurança

da informação, através do estabelecimento de uma política clara e objetiva, alinhada com os objetivos de negócio da organização. A seção 5 apresenta como deve ser desenvolvido, mantido e atualizado o documento da política.

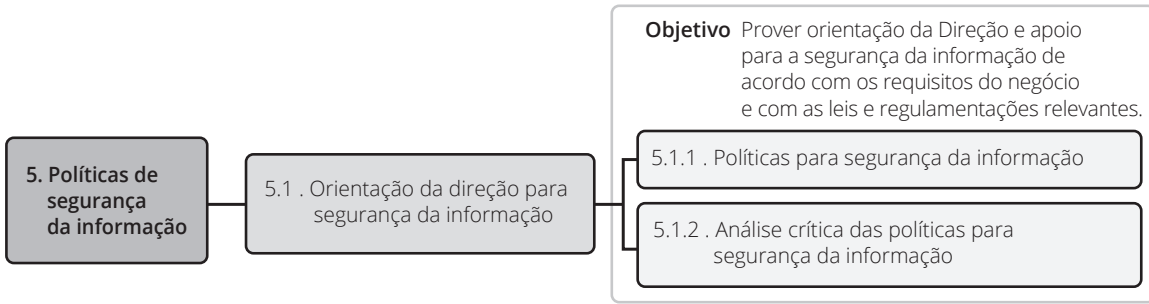


Figura 2.2 Seção 5.1 – Política de segurança da informação.

Essa seção é composta por uma categoria principal de segurança (5.1 – Política de segurança da informação) e por dois controles (5.1.1 e 5.1.2).

O controle 5.1.1 (Políticas para segurança da informação) mostra, nas "Diretrizes para implementação", o que convém que o documento da política contenha e a importância de que ela seja comunicada a todos. Apresenta ainda exemplos de políticas especificas para apoiarem as políticas de segurança da informação.

O controle 5.1.2 (Análise crítica da política de segurança da informação) apresenta como convém que seja realizada a análise crítica pela direção da organização a intervalos planejados ou quando mudanças importantes ocorrerem.

Exercício de fixação 1
Seção 5 – Política de segurança

Utilizando a norma, explique:

O objetivo da categoria de controle 5.1.

A letra b das diretrizes para implementação do controle 5.1.1.

Seção 6 – Organização da segurança da informação

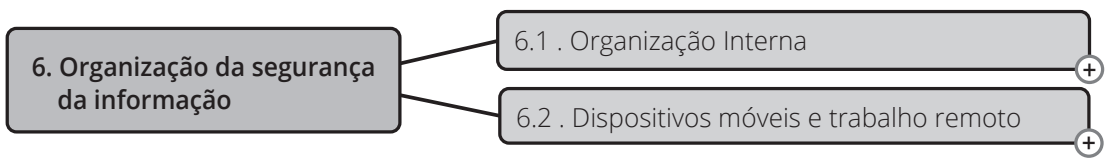


Figura 2.3 Seção 6 - Organização da segurança da informação.

A seção 6 (Organização da segurança da informação) tem como objetivos apresentar controles para uma estrutura para gerenciar a segurança da informação dentro da organização e também os controles para que possa ser mantida a segurança dos recursos de processamento da informação, quando disponibilizados através de dispositivos móveis ou trabalho remoto. Em Informações adicionais do controle 6.2.2, apresenta o entendimento de trabalho remoto segundo a norma 27002:2013.

Na seção 6 encontraremos os controles que devem ser aplicados à estrutura funcional da segurança da informação. A seção 6 possui duas categorias principais de segurança: 6.1 (Organização interna) e 6.2 (Dispositivos móveis e trabalho remoto).

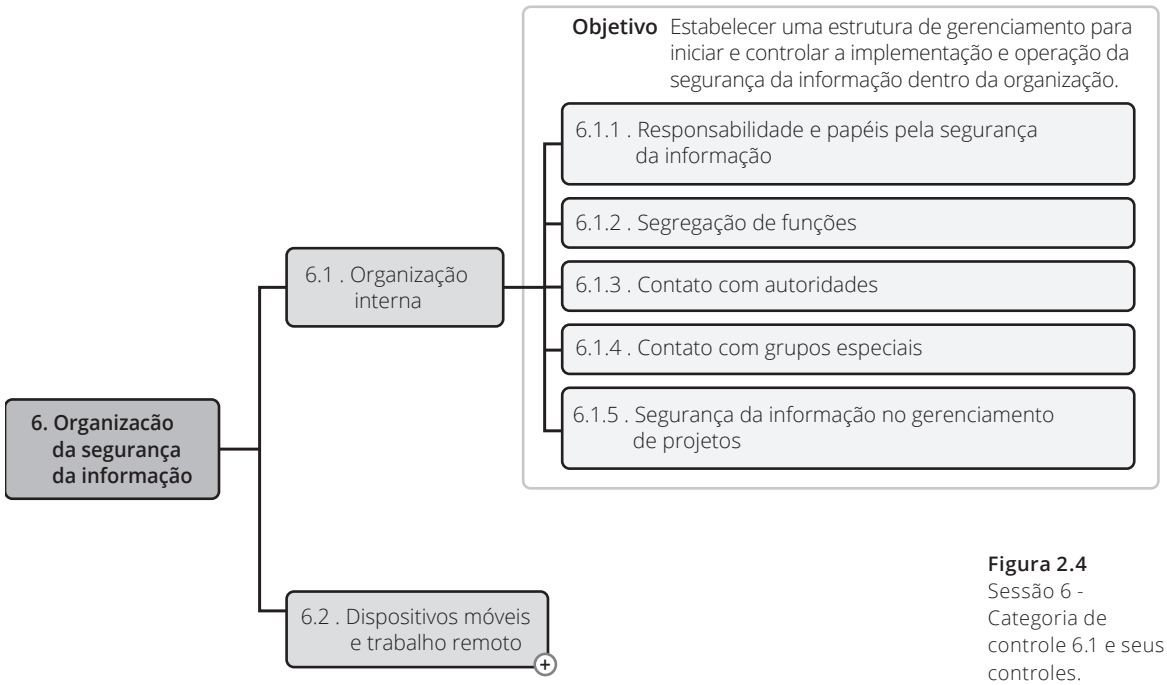


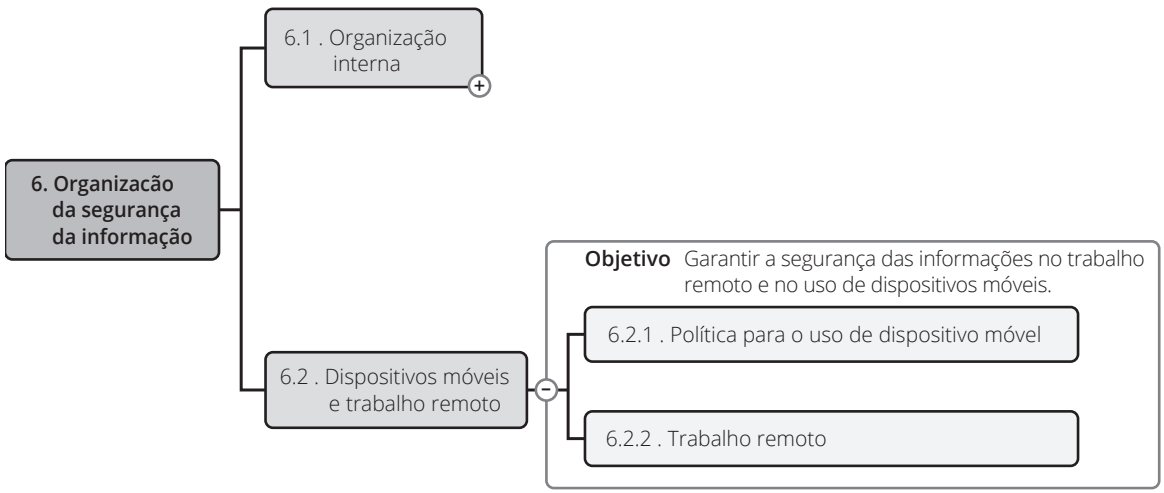
Figura 2.4
Sessão 6 - Categoria de controle 6.1 e seus controles.

A categoria 6.1 (Organização interna) possui cinco controles que devem ser implementados. Esses controles, como podem ser vistos na norma, tratam da estruturação da segurança, seus processos de autorização, confidencialidade e contatos com outros grupos.

Observe que o controle 6.1.5 trata da segurança da informação no gerenciamento de projetos. Independente do tipo de projeto, a norma destaca a importância em se pensar segurança da informação desde o momento inicial. A segurança da informação deve fazer parte de todo o processo, e ser periodicamente analisada, revista e corrigida para estar sempre atualizada com os requisitos de segurança da informação.

Recomendamos uma rápida leitura da categoria 6.1 da norma 27002:2013.

Figura 2.5
Seção 6 – Categoria de controle 6.2 e seus controles.



A categoria 6.2 (Dispositivos móveis e trabalho remoto) trata dos controles necessários para que a organização possa gerenciar a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

Atente para o detalhamento das diretrizes para implementação, que relaciona o essencial a ser observado na segurança da informação.

Exercício de fixação 2
Seção 6 – Organização da segurança da informação

Utilizando a norma, explique os controles:

6.1.2.

6.1.3.

6.1.5.

Seção 7 – Segurança em Recursos Humanos

7.1. Antes da contratação

- Objetivo:
  - Assegurar que os funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados.

7.2. Durante a contratação

- Objetivo:
  - Assegurar que os funcionários e partes externas estejam conscientes e cumpram as suas responsabilidades de segurança da informação.

7.3. Encerramento e mudança da contratação

- Objetivo:
  - Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

A seção 7 (Segurança em Recursos Humanos) trata dos controles de segurança da informação durante o ciclo de vida da prestação de serviços por profissional na organização. Esses controles são organizados pela norma em três categorias:

- 7.1. Antes da contratação;
- 7.2. Durante a contratação;
- 7.3. Encerramento e mudança da contratação.

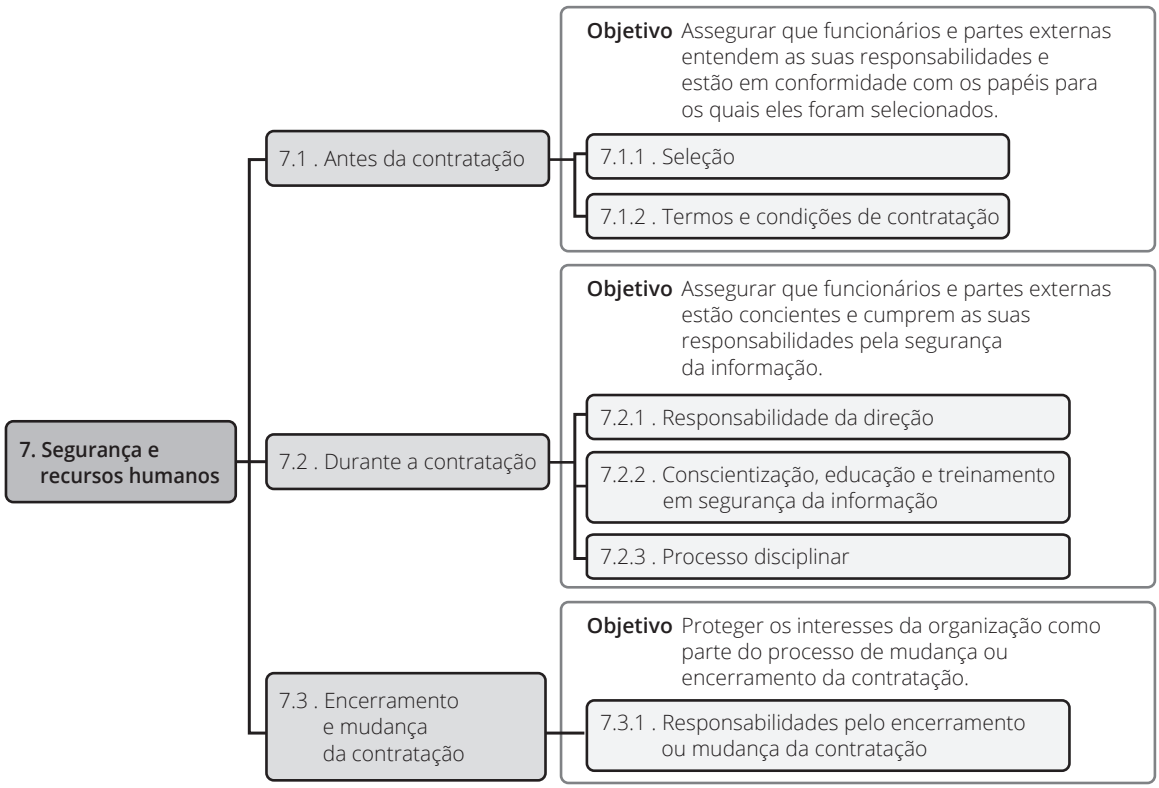


Figura 2.6
Seção 7 - Categorias de controle 7.1, 7.2 e 7.3 com seus controles.

Os controles em cada categoria são organizados dentro das necessidades mínimas de segurança a serem observadas em cada uma delas.

- **Categoria 7.1 (Controles específicos para antes da contratação)**: processo de seleção e condições dos contratos de recursos humanos;
- **Categoria 7.2 (Controles durante a prestação dos serviços propriamente ditos)**: nessa categoria, encontram-se os controles de responsabilidades, de capacitação dos recursos humanos em segurança da informação e do processo disciplinar, caso ocorra uma violação da segurança da informação;
- **Categoria 7.3 (Controles específicos para o encerramento ou mudança de contratação)**: mudança de área, de cargo, promoção, entre outras): nessa categoria destacam-se os controles de devolução de ativos e retirada de direitos de acesso;

Como partes externas entende-se todo aquele que não é efetivamente pertencente aos quadros da organização. Assim, temos como exemplos de partes externas vendedores, fornecedores, agências governamentais, terceirizados, prestadores de serviço temporário e clientes entre outros.

Exercício de fixação 3
Seção 7 – Segurança em Recursos Humanos

Utilizando a norma, explique os controles:

7.1.1.

7.2.2.

7.2.3.

7.3.1.

Seção 8 – Gestão de ativos

8.1. Responsabilidade pelos ativos

- Objetivo:
  - Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

8.2. Classificação das informações

- Objetivo:
  - Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

8.3 Tratamento de mídias

- Objetivo:
  - Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

Na seção 8 (Gestão de ativos) são apresentadas duas categorias de controles de segurança da informação:

- **8.1 (Responsabilidade pelos ativos)**: apresenta os controles que se referem à proteção dos ativos da organização;
- **8.2 (Classificação das informações)**: controles para a classificação da informação, dando a elas um nível adequado de segurança;
- **8.3 (Tratamento de mídias)**: lista os controles para gerenciamento e tratamento das diversas mídias.

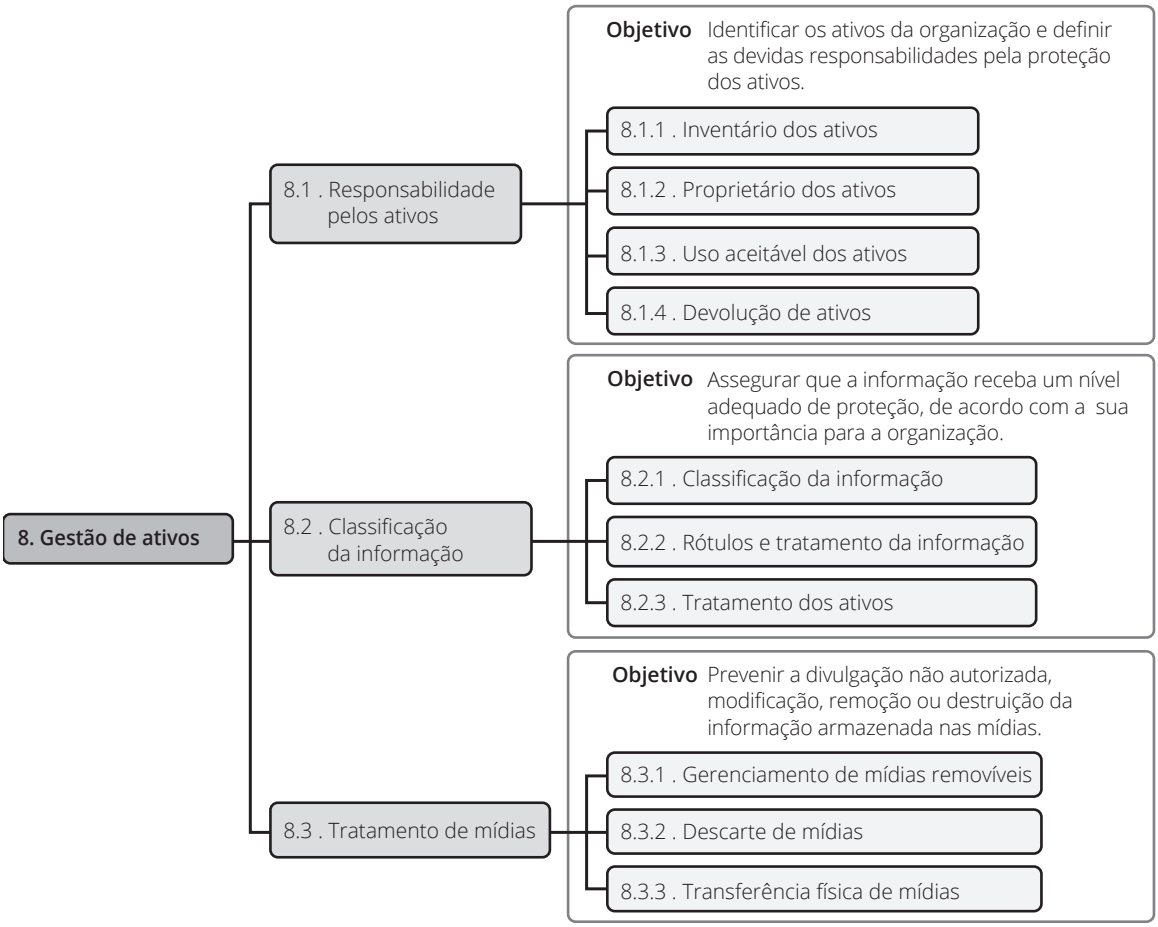


Figura 2.7
Seção 8 - Categorias de controles de segurança 8.1, 8.2 e 8.3 com seus controles.

A categoria 8.1 (Responsabilidade pelos ativos) tem o objetivo de alcançar e manter a proteção adequada dos ativos da organização, apresentando os controles que devem ser aplicados no tratamento da segurança da informação nos ativos. No controle 8.1.1 da norma, em "Informações adicionais", é citada a norma ABNT NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação, na qual são descritos alguns tipos de ativos.

Já a categoria 8.2 apresenta os controles para a classificação da informação que devem ser aplicados e a importância dessa atividade para a gestão de ativos.

Na categoria 8.3 são listados os controles e diretrizes necessários ao tratamento das mídias.

Para mais informações sobre classificação da informação leia a ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação, e também o Decreto Nº 7.845, de 14 de novembro de 2012).

Exercício de fixação 4
Seção 8 – Gestão de ativos

Utilizando a norma, explique os controles:

8.1.1.

_____

_____

_____

Saiba mais

Consulte as normas ABNT NBR ISO 55000:2014 – Gestão de ativos – Visão geral, princípios e terminologia e ABNT NBR ISO 55001:2014 – Gestão de ativos – Sistemas de gestão – Requisitos.

8.1.2.

8.2.1.

8.3.2.

Seção 9 – Controle de acesso

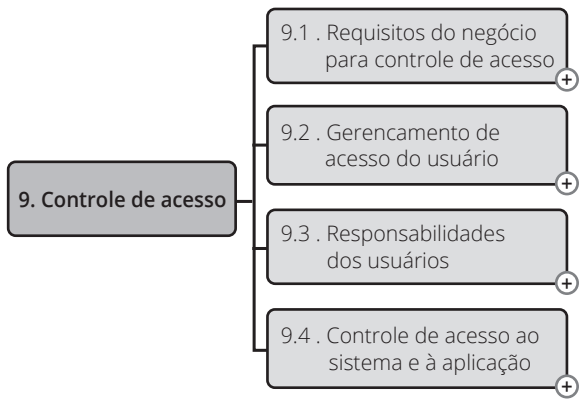


Figura 2.8
Seção 9 e suas quatro categorias de controles de segurança.

Na seção 9 (Controle de acesso) são encontradas as categorias que tratam dos controles necessários ao controle de acesso lógico. Diferentemente da seção 11 (Segurança física e do ambiente), na seção 9 são tratados aspectos relativos a privilégios de acesso, senhas, acesso a rede, entre outros. Nessa seção existem quatro categorias de controles de segurança.

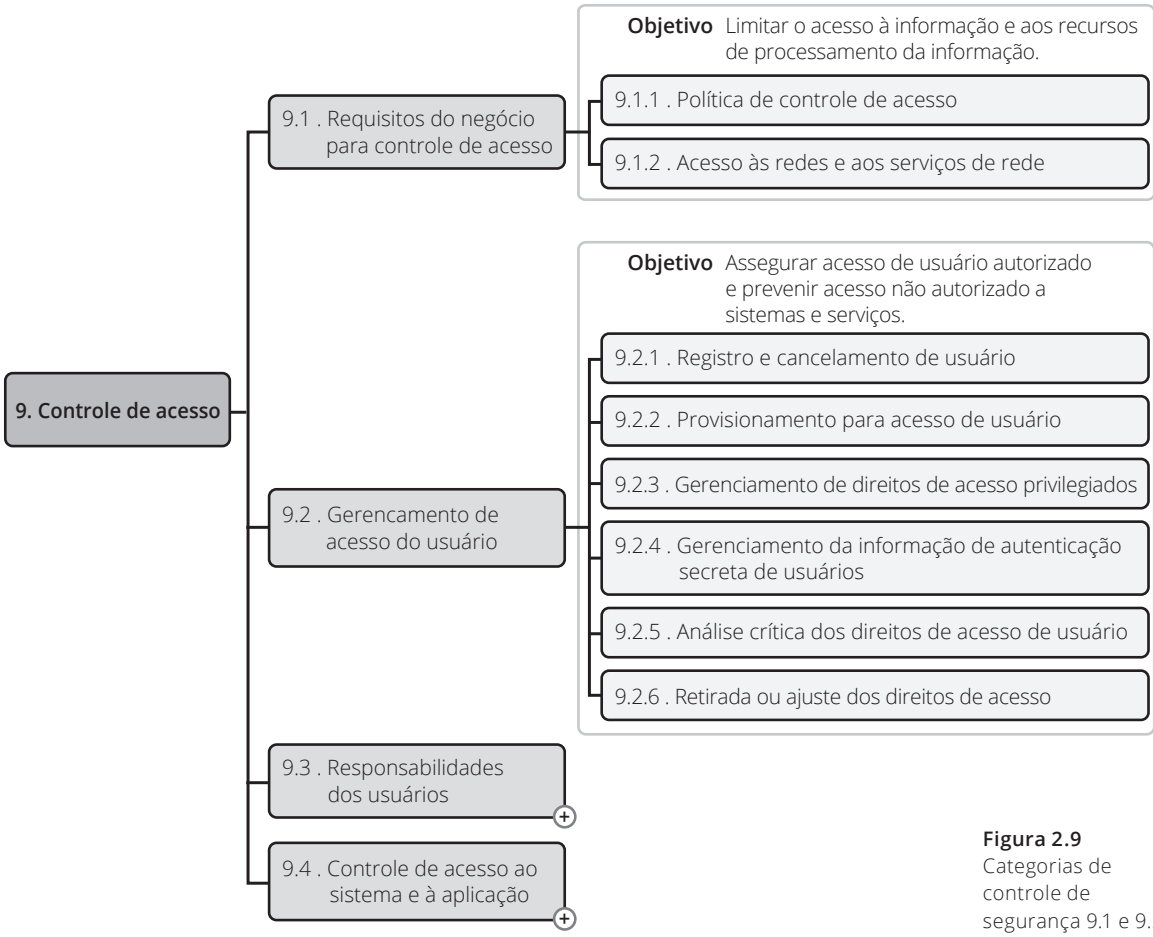


Figura 2.9
Categorias de controle de segurança 9.1 e 9.2 com seus controles

Na categoria 9.1 (Requisitos de negócio para controle de acesso), o objetivo é limitar o acesso à informação e aos recursos de processamento da informação.

A categoria 9.2 (Gerenciamento de acesso do usuário) tem por objetivo assegurar o acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços. Os controles são:

- **9.2.1 (Registro de usuário)**: descreve a conveniência da existência de um procedimento formal de registro e cancelamento de usuário;
- **9.2.2 (Provisionamento para acesso de usuário)**: apresenta a necessidade de um processo formal de provisionamento de acesso;
- **9.2.3 (Gerenciamento de direitos de acesso privilegiados)**: apresenta a necessidade de que a concessão de senhas seja controlada;
- **9.2.4 (Gerenciamento da informação de autenticação secreta de usuários)**: destaca que a concessão de informação de autenticação seja controlada por um processo de gerenciamento formal;
- **9.2.5 (Análise crítica dos direitos de acesso de usuário)**: apresenta a conveniência do gestor conduzir análises críticas periódicas dos direitos de acesso;
- **9.2.6 (Retirada ou ajuste dos direitos de acesso)**: apresenta a importância da retirada dos acessos logo após o encerramento das atividades dos funcionário e partes externas.

A categoria 9.3 (Responsabilidades dos usuários) objetiva tornar os usuários responsáveis pela proteção das suas informações de autenticação. Possui o controle:

- **9.3.1 (Uso da informação de autenticação)**: trata da necessidade de os usuários seguirem as boas práticas no uso da informação secreta;

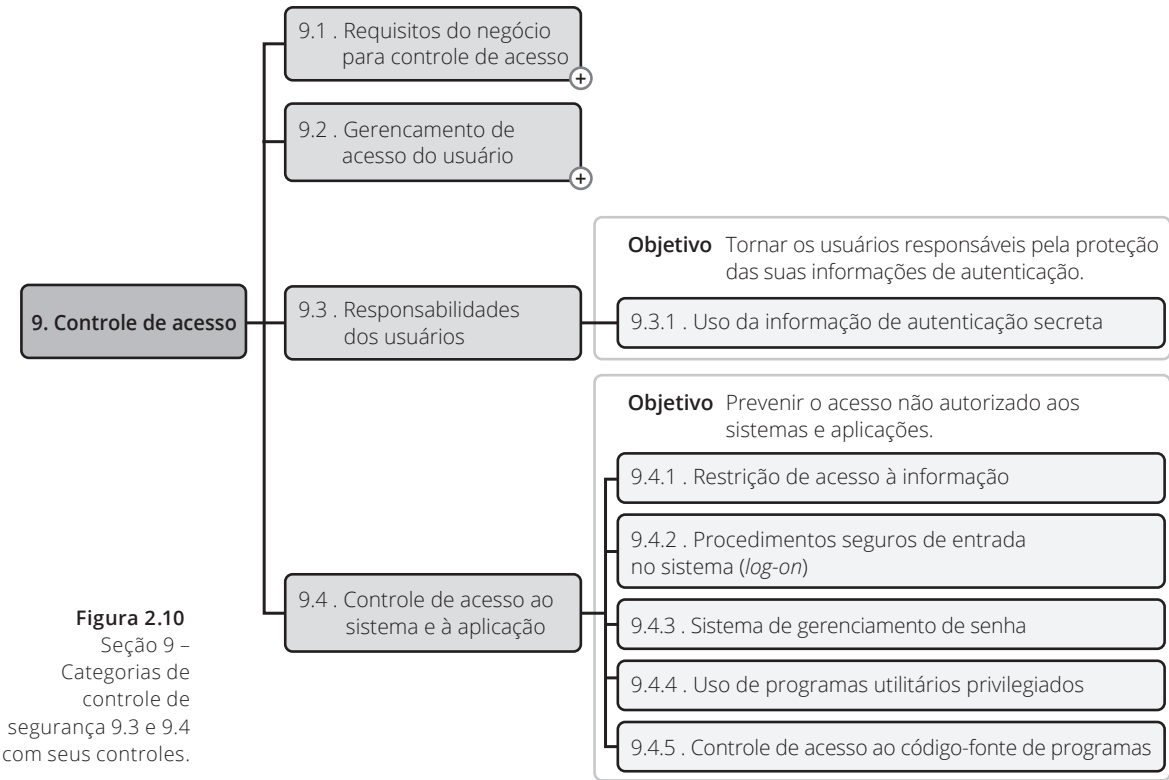


Figura 2.10
Seção 9 – Categorias de controle de segurança 9.3 e 9.4 com seus controles.

A categoria 9.4 (Controle de acesso ao sistema e à aplicação) tem como objetivo prevenir o acesso não autorizado aos sistemas e aplicações. Possui os seguintes controles:

- **9.4.1 (Restrição de acesso à informação)**: apresenta a conveniência de que os usuários recebam acesso somente aos serviços que tenham sido autorizados a usar;
- **9.4.2 (Procedimentos seguros de entrada no sistema – log on)**: apresenta a conveniência de que o sistema sejam controlado por um procedimento seguro;
- **9.4.3 (Sistema de gerenciamento de senha)**: apresenta a conveniência de que os sistemas de gerenciamento de senhas assegurem senhas de qualidade;
- **9.4.4 (Uso de programas utilitários privilegiados)**: destaca a importância de se ter sob controle programas utilitários que possam sobrepor os controles dos sistemas e aplicações;
- **9.4.5 (Controle de acesso ao código-fonte de programas)**: apresenta a conveniência da restrição de acesso ao código-fonte.

Exercício de fixação 5
Seção 9 – Controle de acessos

Utilizando a norma, explique os controles:

9.1.1.

9.2.2.

9.2.4.

9.2.6.

9.4.2.

Seção 10 – Criptografia

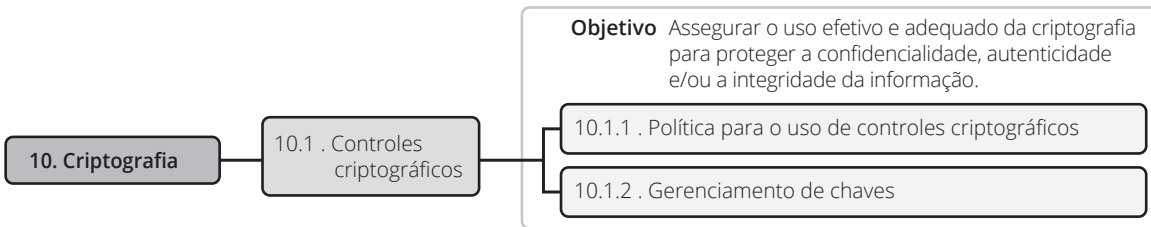


Figura 2.11
Seção 10 e sua categoria de controle de segurança.

A seção 10 (Criptografia) possui a categoria 10.1, Controles criptográficos, que tem como objetivo assegurar o uso efetivo e adequado da criptografia. Os controles são:

- **10.1.1 (Política para o uso de controles criptográficos)**: convém ter uma política sobre o uso de controles criptográficos.
- **10.1.2 (Gerenciamento de chaves)**: apresenta a conveniência do uso, proteção e tempo de vida das chaves criptográficas.

Exercício de fixação 6
Seção 10 – Criptografia

Utilizando a norma, explique os controles:

10.1.1.

10.1.2.

Seção 11 – Segurança física e do ambiente

11.1. Áreas seguras

- Objetivo:
  - Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização.

9.2. Equipamento

- Objetivo:
  - Impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das operações da organização.

Tendo como objetivo o tratamento da segurança física e do ambiente, a seção 11 (Segurança física e do ambiente) apresenta duas categorias principais de segurança da informação:

- 11.1. Áreas seguras;
- 11.2. Equipamento.

Os controles de segurança da categoria 11.1 (Áreas seguras) tratam especificamente das necessidades de segurança de acesso físico às instalações. São apresentados controles de segurança para o perímetro físico, controles de entrada nas áreas internas e externas, áreas seguras, áreas com acesso público e de entrega de material.

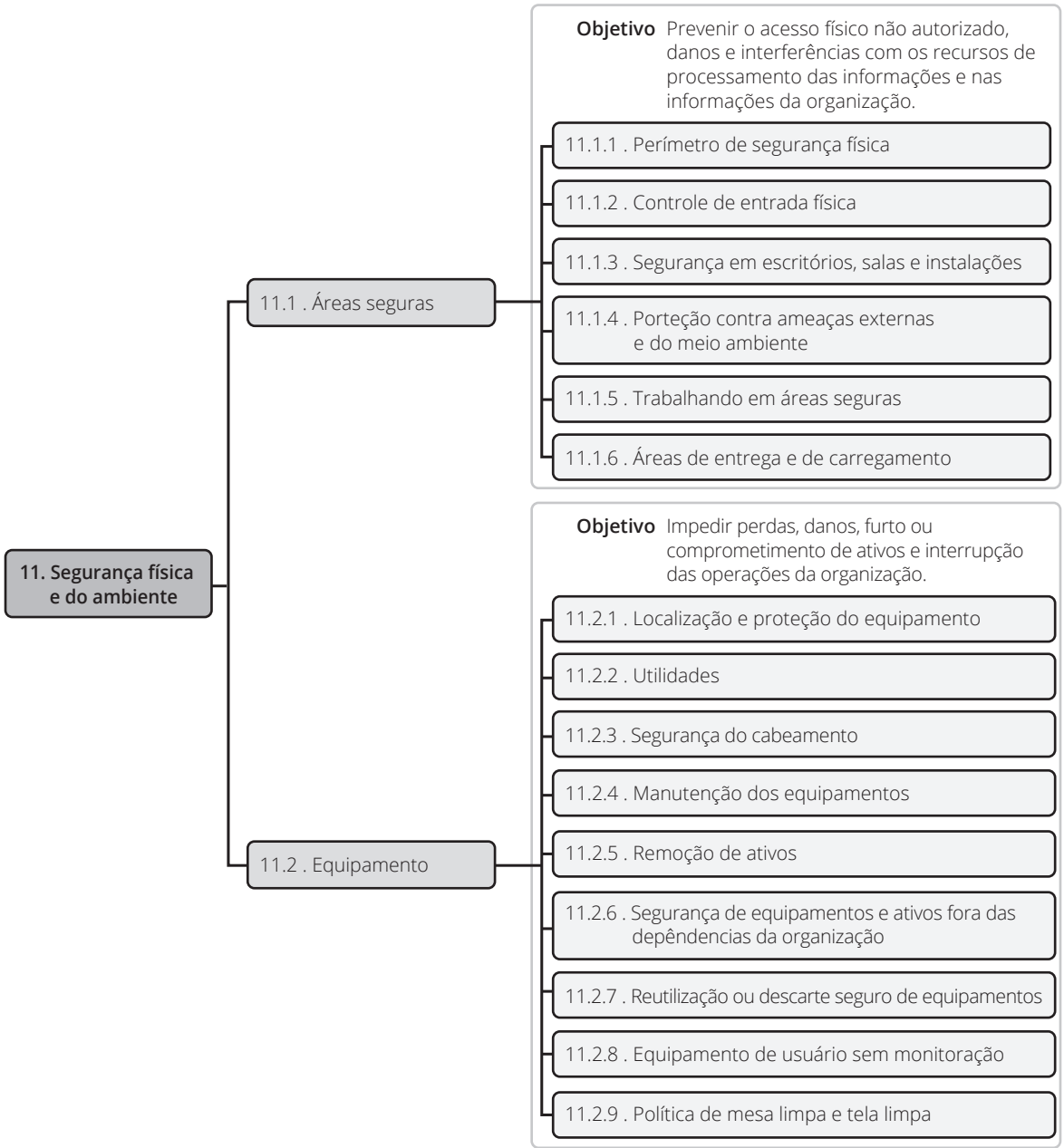


Figura 2.12 Seção 11 – Categorias de controle de segurança 11.1 e 11.2 com seus controles.

Na categoria 11.2 (Equipamento) estão os controles de segurança que se referem à proteção física dos ativos e ao seu funcionamento sem interrupções. É nesta categoria que se encontram os controles para a instalação de equipamentos, fornecimento de energia, ar-condicionado, manutenção dos ativos, reutilização e venda/alienação de ativos.

Exercício de fixação 7

Seção 11 – Segurança física e do ambiente

Utilizando a norma, explique os controles:

11.1.2.

11.1.4.

11.2.5.

11.2.9.

Seção 12 – Segurança nas operações

- 12.1. Responsabilidade e procedimentos operacionais.
- 12.2. Proteção contra malware.
- 12.3. Cópias de segurança.
- 12.4. Registros e monitoramento.
- 12.5. Controle de software operacional.
- 12.6. Gestão de vulnerabilidades técnicas.
- 12.7. Considerações quanto à auditoria de sistema da informação.

A seção 12 (Segurança nas operações) é a seção da norma que trata das operações dos serviços tecnológicos da organização. Essa seção possui sete categorias de controle de segurança da informação, e cada uma delas apresenta controles que convêm serem aplicados no dia a dia das operações e comunicações da organização. É a seção que apresenta os controles de segurança que atendem à maioria das vulnerabilidades relativas a aspectos operacionais do cotidiano da área de TIC.

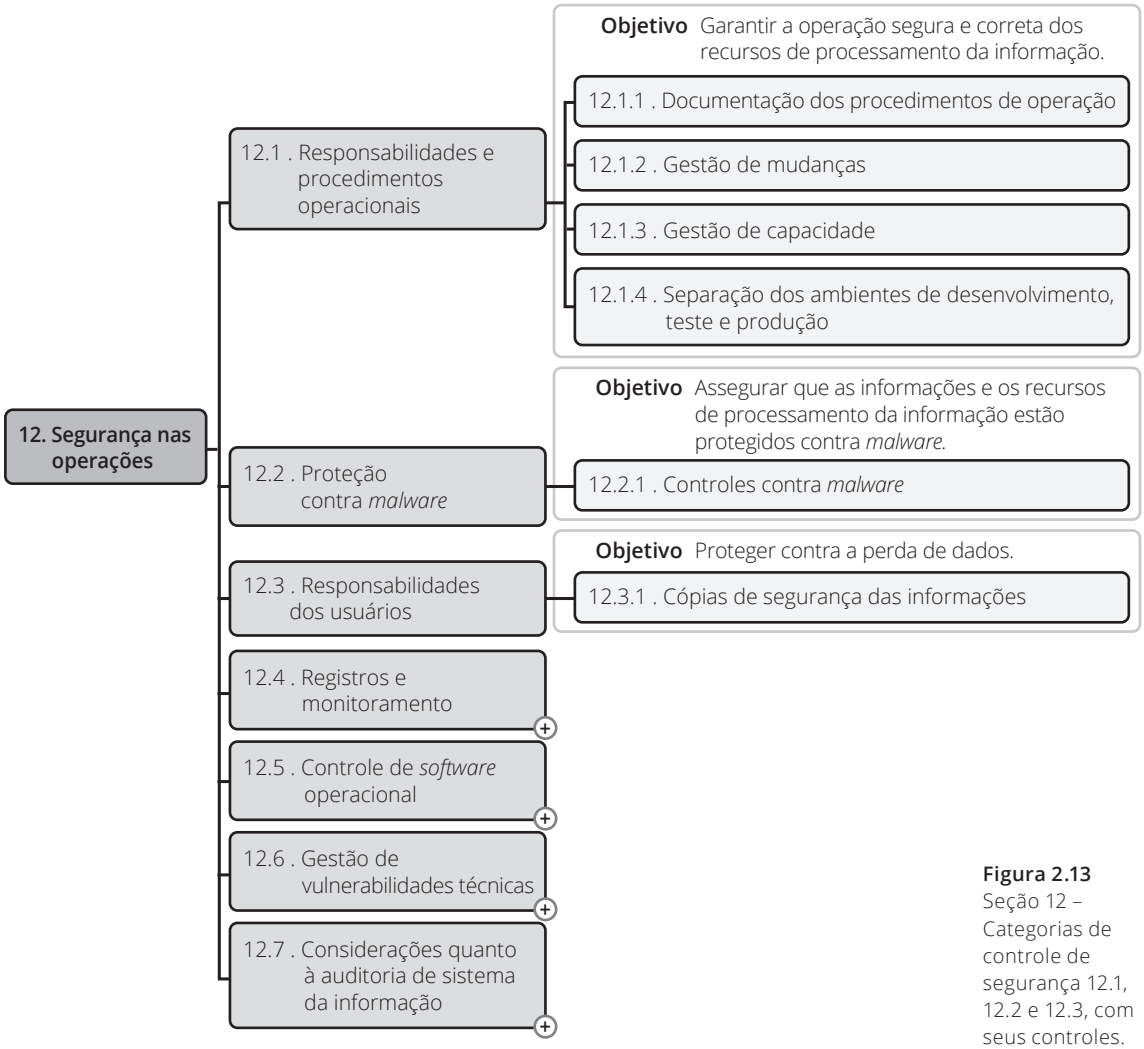


Figura 2.13
Seção 12 – Categorias de controle de segurança 12.1, 12.2 e 12.3, com seus controles.

Na categoria 12.1 (Responsabilidades e procedimentos operacionais) são mostrados os controles que buscam garantir a operação segura e correta dos recursos computacionais. Nela são descritos os controles:

- **12.1.1 (Documentos dos procedimentos de operação)**: devem ser aplicados para documentar os procedimentos;
- **12.1.2 (Gestão de mudanças)**: define como devem ser controladas as modificações e alterações;
- **12.1.3 (Gestão de capacidade)**: trata do monitoramento e sincronização dos recursos com as projeções de capacidade futura para garantir o desempenho requerido;
- **12.1.4 (Separação dos ambientes de desenvolvimento, teste e produção)**: descreve como esses ambientes devem ser separados para reduzir o risco de acessos ou modificações não autorizadas.

A categoria 12.2 (Proteção contra malware) tem como um dos objetivos manter o nível de segurança adequado e das entregas de serviços em consonância com os acordos. Essa categoria possui os seguintes controles:

- **12.2.1 (Controles contra malware)**: trata de controles de detecção e prevenção para proteger contra malware junto com um programa de conscientização do usuário.

Na categoria 12.3 (Cópias de segurança), o objetivo é proteger contra a perda de dados, mantendo a integridade e disponibilidade da informação, através do seguinte controle:

- **12.3.1 (Cópias de segurança das informações)**: trata da necessidade de que cópias de segurança (backup) das informações e dos softwares sejam efetuadas e testadas regularmente.

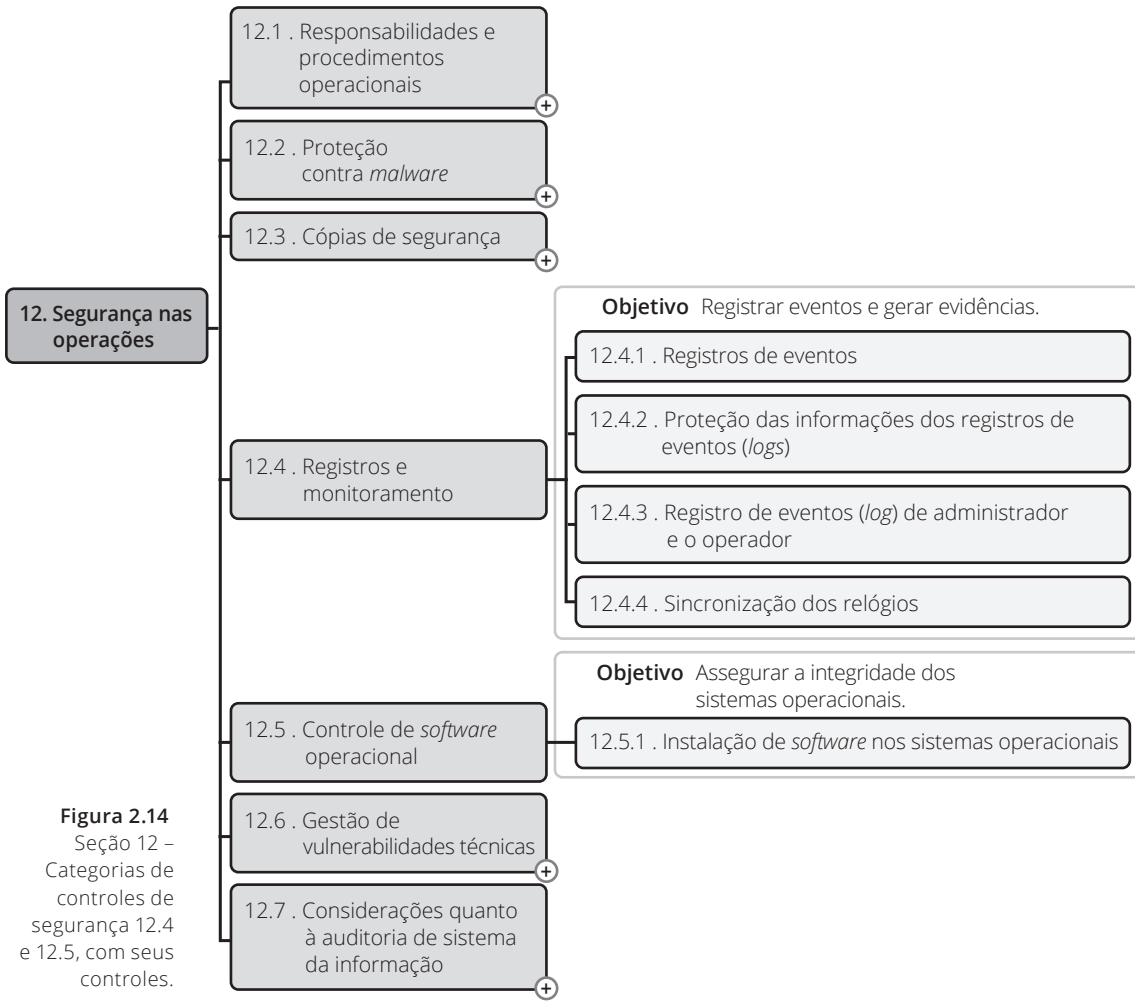


Figura 2.14 Seção 12 – Categorias de controles de segurança 12.4 e 12.5, com seus controles.

A categoria 12.4 (Registros e monitoramento) tem por objetivo detectar atividades não autorizadas de processamento da informação de forma a registrar eventos e gerar evidências. Os controles são:

- **12.4.1 (Registros de eventos)**: onde são descritos os procedimentos para o registro dos logs de eventos;
- **12.4.2 (Proteção das informações dos registros de eventos – logs)**: mostra as diretrizes para a proteção dos logs contra acesso não autorizado e adulteração.
- **12.4.3 (Registros de eventos – log – de administrador e operador)**: convém que as atividades dos administradores e operadores do sistema sejam registradas;
- **12.4.4 (Sincronização dos relógios)**: convém que todos os sistemas relevantes tenham seus relógios sincronizados.

Na categoria 12.5 (Controle de software operacional), o objetivo é manter a integridade e disponibilidade dos Sistemas Operacionais, através do seguinte controle:

- **12.5.1 (Instalação de software nos Sistemas Operacionais)**: trata da necessidade da implementação de procedimentos para controlar a instalação de software em sistemas operacionais.

A categoria 12.6 (Gestão de vulnerabilidades técnicas) objetiva prevenir a exploração de vulnerabilidades técnicas. Essa categoria possui dois controles:

- **12.6.1 (Gestão de vulnerabilidades técnicas)**: trata da necessidade do gerenciamento e controle das vulnerabilidades técnicas em tempo hábil;
- **12.6.2 (Restrições quanto a instalação de software)**: descreve a necessidade de definição de regras e critérios para a instalação de software pelo usuário.

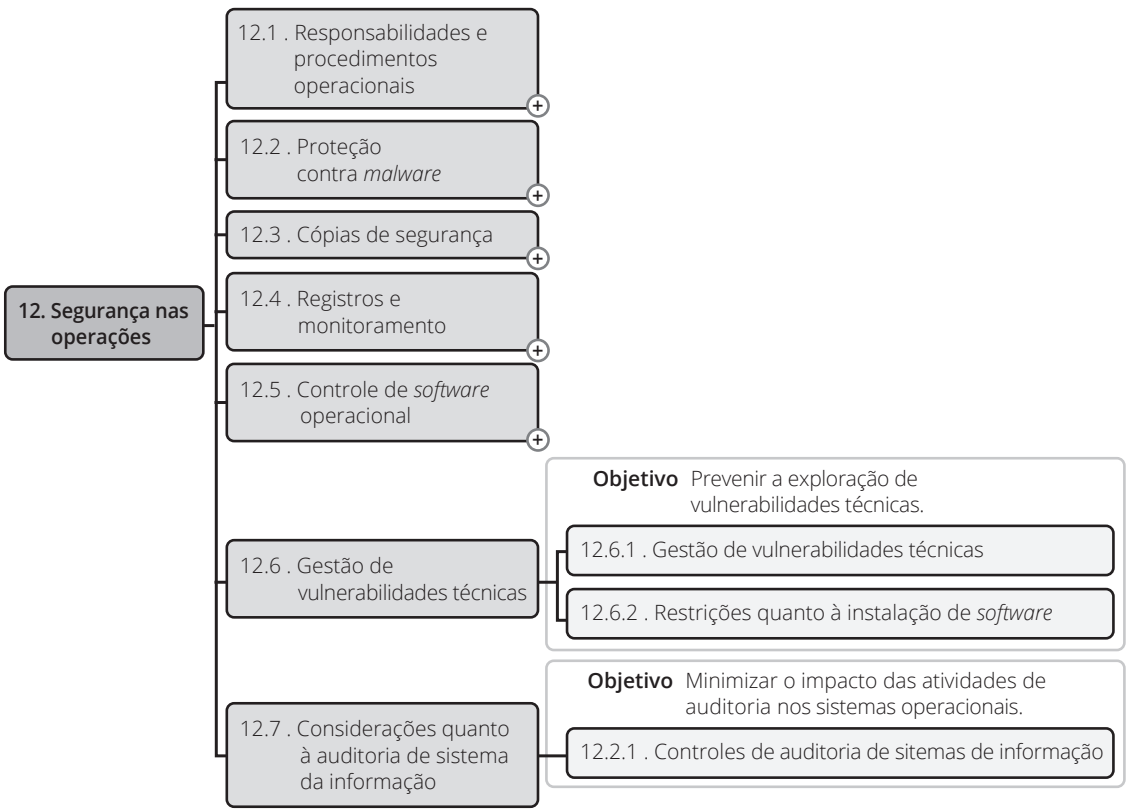


Figura 2.15 Seção 12 – Categorias de controles de segurança 12.6 e 12.7, com seus controles.

Na categoria 12.7 (Considerações quanto à auditoria de sistemas da informação), é descrito o controle que deve ser aplicado para minimizar o impacto das atividades de auditoria nos Sistemas Operacionais:

- **12.7.1 (Controles de auditoria de sistemas de informação)**: descreve as atividades e requisitos de auditoria para que sejam planejados cuidadosamente.

Exercício de fixação 8
Seção 12 – Segurança nas operações

Utilizando a norma, explique os controles:

12.1.3.

12.2.2.

12.4.1.

12.5.1.

12.6.2.

12.7.1.

12.4.3.

Seção 13 – Segurança nas comunicações

Na seção 13 (Segurança nas comunicações), são encontradas as categorias que tratam dos controles necessários para a segurança das comunicações. Nesta seção existem duas categorias principais de segurança.

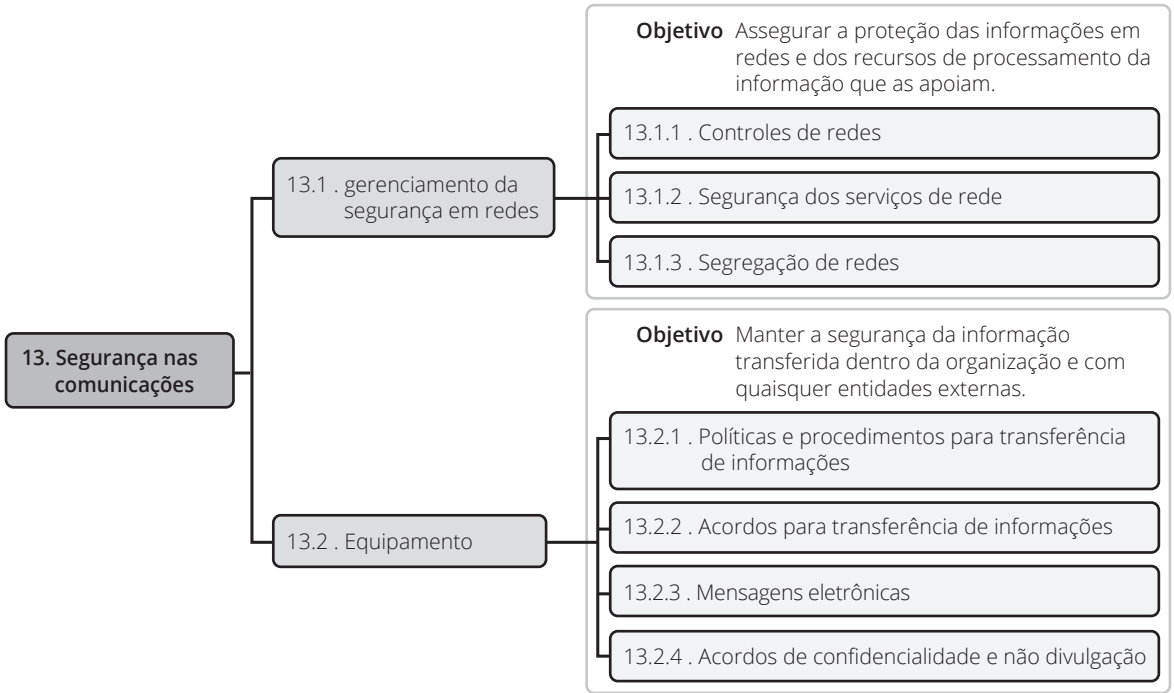


Figura 2.16 Seção 13 - Categorias de controle de segurança 13.2 e 13.1 com seus controles.

A categoria 13.1 (Gerenciamento da segurança em redes) objetiva garantir a proteção das informações em redes e a proteção da infraestrutura de suporte. Essa categoria possui três controles:

- **13.1.1 (Controle de redes)**: trata da necessidade do gerenciamento e controle adequado das redes, incluindo a informação em trânsito;
- **13.1.2 (Segurança dos serviços de rede)**: descreve a necessidade de que os níveis de serviços de rede sejam identificados e incluídos nos acordos de níveis de serviço.
- **13.1.3 (Segregação de redes)**: apresenta a importância da segregação em redes dos diversos grupos.

A categoria 13.2 (Transferência de informação) objetiva manter a segurança na troca de informações internamente e com entidades externas. Possui os seguintes controles:

- **13.2.1 (Políticas e procedimentos para transferência de informações)**: convém que sejam estabelecidas políticas e procedimentos para a proteção da troca de informações;
- **13.2.2 (Acordos para a troca de informações)**: convém estabelecer acordos para a troca de informações;
- **13.2.3 (Mensagens eletrônicas)**: convém que as mensagens sejam devidamente protegidas;
- **13.2.4 (Acordos de confidencialidade e não divulgação)**: convém que os requisitos para confidencialidade ou acordos de não divulgação sejam identificados e analisados.

Exercício de fixação 9
Seção 13 – Segurança nas comunicações

Utilizando a norma, explique os controles:

13.1.1.

13.1.2.

13.1.3.

13.2.1.

13.2.4.

Seção 14 – Aquisição, desenvolvimento e manutenção de sistemas

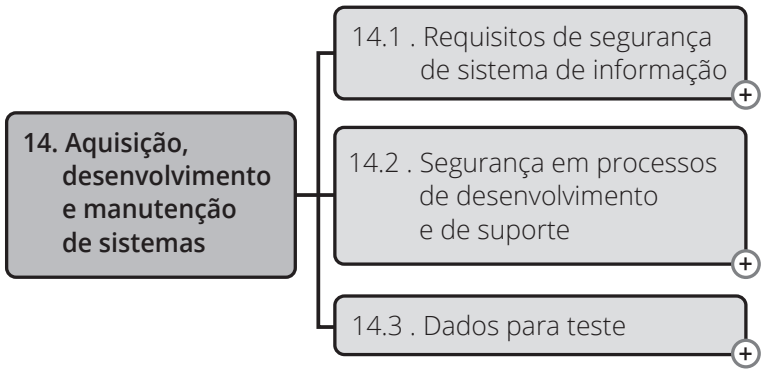
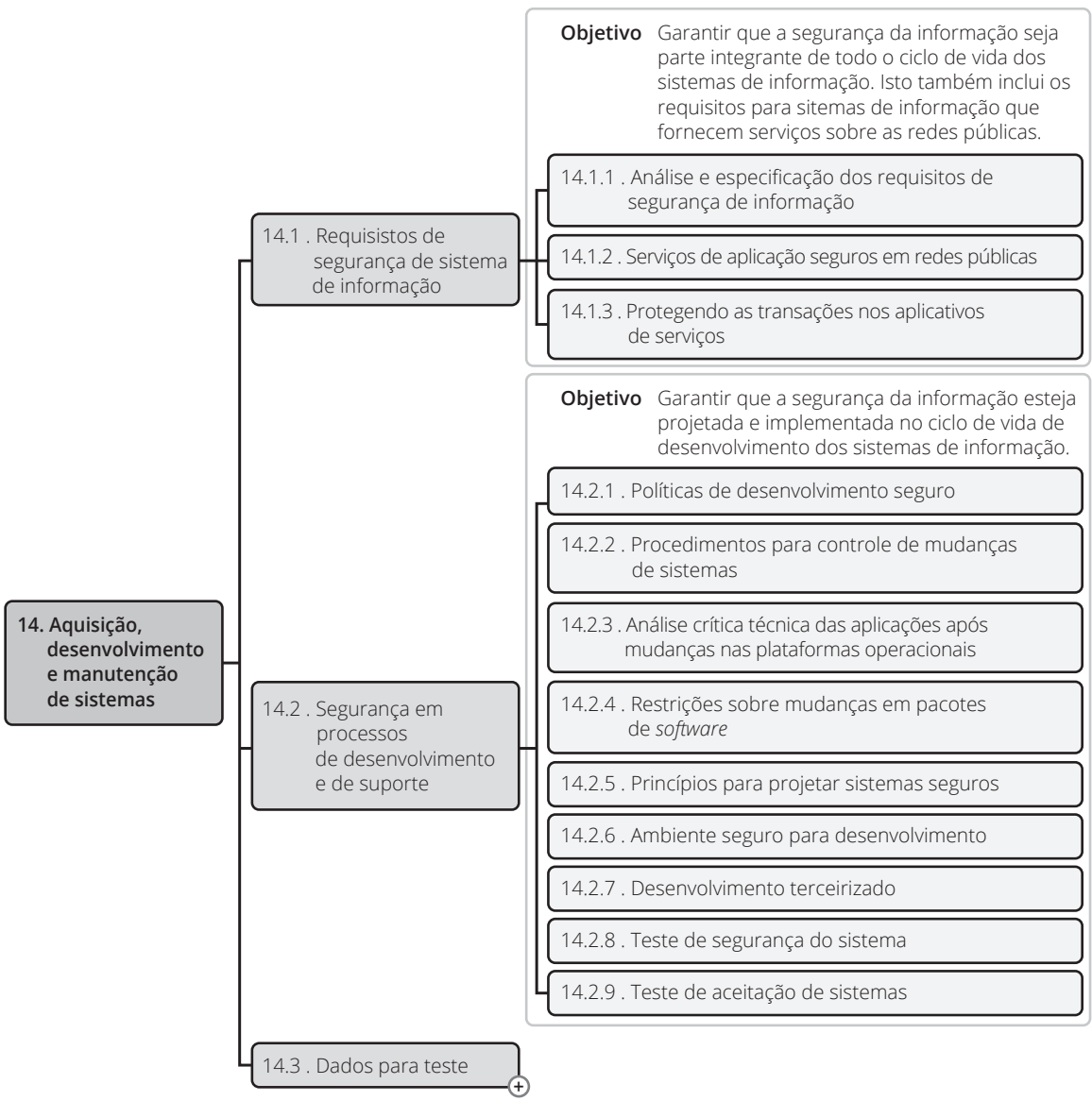


Figura 2.17
Seção 12 com suas três categorias principais de segurança.

Na seção 14 (Aquisição, desenvolvimento e manutenção de sistemas de informação) estão os controles relativos às atividades de aquisição, desenvolvimento e manutenção de softwares. O objetivo nesta seção é desenvolver a segurança da informação nos aplicativos da organização. Esta seção possui 6 categorias principais de segurança.

Figura 2.18
Categorias principais de segurança 14.1 e 14.2 com seus controles.



A categoria 14.1 (Requisitos de segurança de sistemas de informação) tem por objetivo garantir que a segurança é parte integrante dos sistemas de informação. Possui o seguinte controle:

- **14.1.1 (Análise e especificação dos requisitos de segurança)**: define procedimentos de segurança nas aplicações que transitam sobre redes públicas;
- **14.1.2 (Serviços de aplicação seguros em redes públicas)**: define controles de segurança nas especificações de requisitos de novos sistemas.

A categoria 14.2 (Segurança em processos de desenvolvimento e de suporte) tem como objetivo manter a segurança de sistemas aplicativos e da informação. Possui os controles:

- **14.2.1 (Política de desenvolvimento seguro)**: aborda a necessidade de que sejam estabelecidas regras para o desenvolvimento de sistemas;
- **14.2.2 (Procedimentos para controle de mudanças de sistemas)**: convém que a implementação de mudanças seja controlada com a utilização de procedimentos formais de controle de mudanças;
- **14.2.3 (Análise crítica técnica das aplicações após mudanças nas plataformas operacionais)**: apresenta a conveniência de que aplicações críticas sejam analisadas criticamente e testadas quando Sistemas Operacionais são mudados;
- **14.2.4 (Restrições sobre mudanças em pacotes de software)**: apresenta a conveniência de que todas as mudanças sejam estritamente controladas;
- **14.2.5 (Princípios para projetar sistemas seguros)**: cita que princípios para projetar sistemas seguros sejam estabelecidos e documentados;
- **14.2.6 (Ambiente seguro para desenvolvimento)**: apresenta a necessidade das organizações estabeleçam ambientes seguros de desenvolvimento;
- **14.2.7 (Desenvolvimento terceirizado)**: convém que a organização supervisione e monitore o desenvolvimento terceirizado de softwares;
- **14.2.8 (Teste de segurança do sistema)**: apresenta a necessidade de que testes de funcionalidade de segurança sejam realizados durante o desenvolvimento.
- **14.2.9 (Teste de aceitação de sistemas)**: Convém que programas de testes de aceitação sejam estabelecidos.

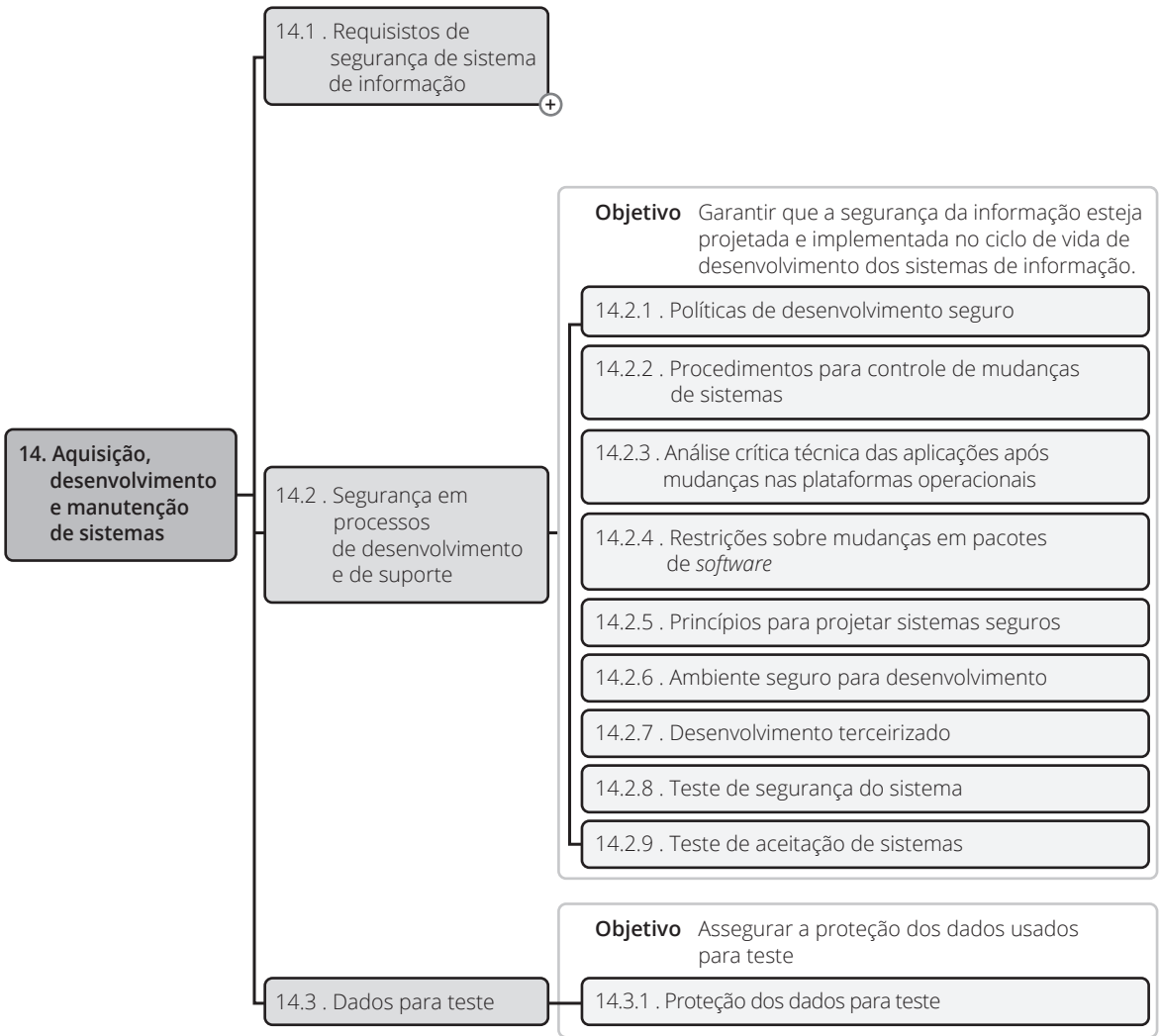


Figura 2.19 Seção 12 – Categorias principais de segurança 14.2 e 14.3, com seus controles.

A categoria 14.3 (Dados para teste) tem como objetivo assegurar a proteção dos dados para teste. O controle é:

- **14.3.1 (Proteção dos dados para teste)**: convém que os dados de teste sejam selecionados e controlados.

Exercício de fixação 10
Seção 14 – Aquisição, desenvolvimento e manutenção de sistemas

Utilizando a norma, explique os controles:

14.1.1.

14.1.2.

14.2.1.

14.2.7.

14.3.1.

Seção 15 – Relacionamento na cadeia de suprimento

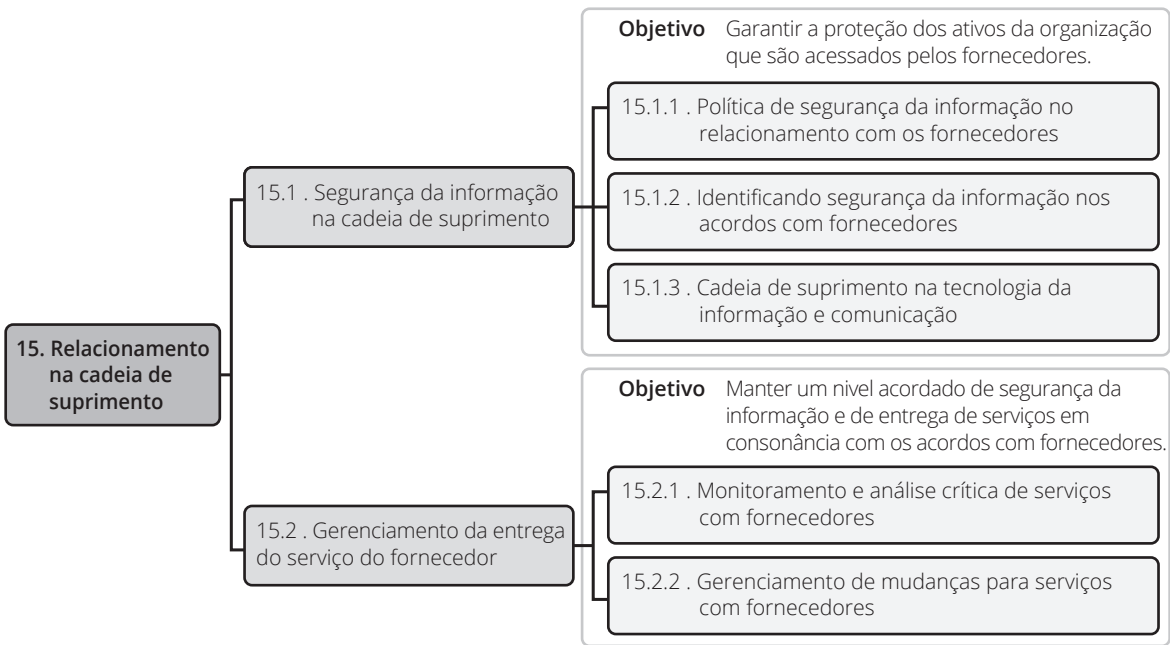


Figura 2.20
Seção 15 com suas duas categorias de controle de segurança e controles.

A seção 15 (Relacionamento na cadeia de suprimento) trata do processo de segurança nos relacionamentos com os fornecedores . Possui duas categorias principais de segurança.

A categoria 15.1 (Segurança da informação na cadeia de suprimento) tem por objetivo assegurar a proteção dos ativos da organização acessados pelos fornecedores. Possui os controles:

- **15.1.1 (Política de segurança da informação no relacionamento com fornecedores)**: define que sejam acordados e documentados os requisitos de segurança para mitigar os riscos;
- **15.1.2 (Identificando segurança da informação nos acordos com fornecedores)**: convém que todos os requisitos de segurança da informação sejam estabelecidos e acordados com cada fornecedor.
- **15.1.3 (Cadeia de suprimento na tecnologia da informação e comunicação)**: convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança.

A categoria 15.2 (Gerenciamento da entrega do serviço do fornecedor) tem por objetivo manter o nível acordado de segurança e de entrega em consonância com os acordos com fornecedores. Os controles são:

- **15.2.1 (Monitoramento e análise crítica de serviços com fornecedores)**: apresenta a conveniência de auditar e analisar criticamente a entrega dos serviços executados;
- **15.2.2 (Gerenciamento de mudanças para serviços com fornecedores)**: apresenta a necessidade de gerenciar as mudanças no provisionamento dos serviços pelos fornecidores.

Exercício de fixação 11
Seção 15 – Relacionamento na cadeia de suprimento

Utilizando a norma, explique os controles:

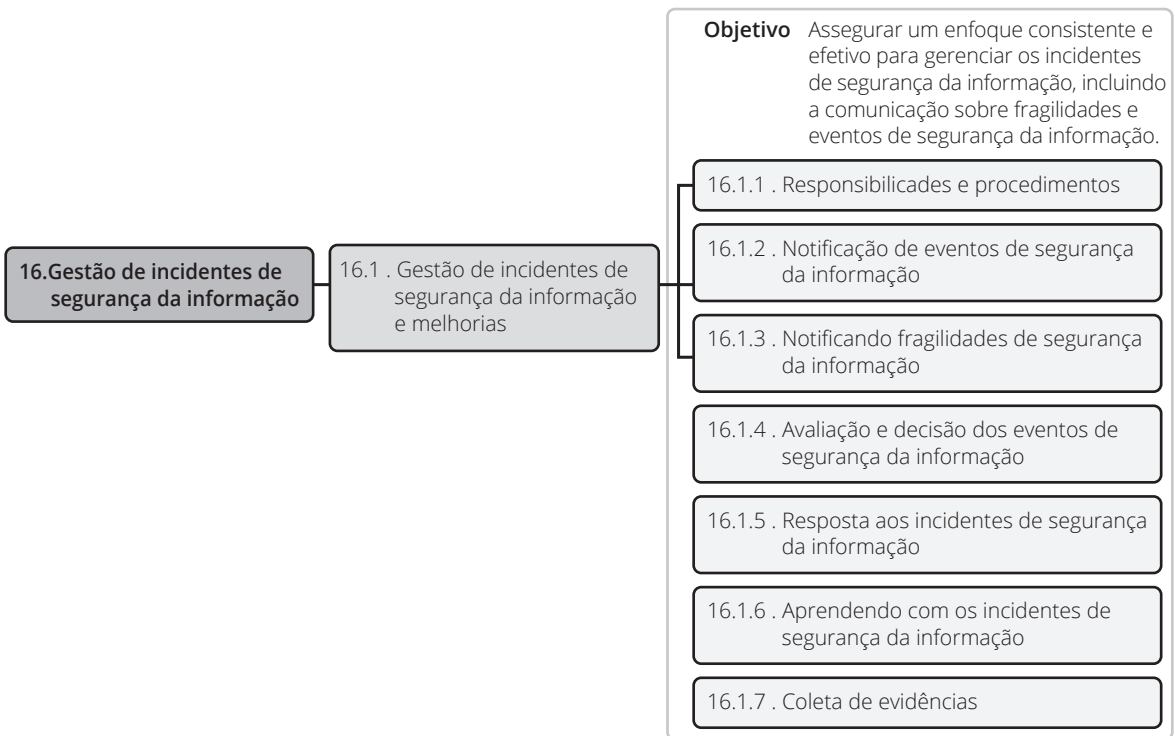
15.1.1.

15.1.2.

15.2.1

Seção 16 – Gestão de incidentes de segurança da informação

Figura 2.21
Seção 16, com suas categorias principais de segurança e controles.



A seção 16 (Gestão de incidentes de segurança da informação) trata do processo de notificação de eventos de segurança, responsabilidades e coleta de evidências. Possui duas categorias principais de segurança.

A categoria 16.1 (Gestão de incidentes de segurança da informação e melhorias) tem por objetivo assegurar que fragilidades e eventos de segurança sejam comunicados, permitindo a tomada de ação corretiva em tempo real. Possui os controles:

- **16.1.1 (Responsabilidades e procedimentos)**: apresenta a conveniência de que responsabilidades e procedimentos sejam estabelecidos para assegurar respostas rápidas;
- **16.1.2 (Notificação de eventos de segurança da informação)**: define que os eventos de segurança sejam relatados através dos canais apropriados o mais rapidamente possível;
- **16.1.3 (Notificando fragilidades de segurança da informação)**: convém que todos os recursos humanos sejam instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas e serviços;
- **16.1.4 (Avaliação e decisão dos eventos de segurança da informação)**: apresenta que os eventos de segurança sejam avaliados e classificados como incidentes;
- **16.1.5 (Resposta aos incidentes de segurança da informação)**: define que devem existir procedimentos documentados para que os incidentes sejam reportados;
- **16.1.6 (Aprendendo com os incidentes de segurança da informação)**: apresenta a conveniência de que sejam estabelecidos mecanismos para quantificar e monitorar os tipos e custos dos incidentes;
- **16.1.7 (Coleta de evidências)**: apresenta a necessidade de que evidências sejam coletadas, armazenadas e apresentadas em conformidade com a legislação pertinente.

Exercício de fixação 12
Seção 16 – Gestão de incidentes de segurança da informação

Utilizando a norma, explique os controles:

16.1.1.

16.1.2.

16.1.5

16.1.7

Seção 17 – Aspectos da segurança da informação na gestão da continuidade do negócio

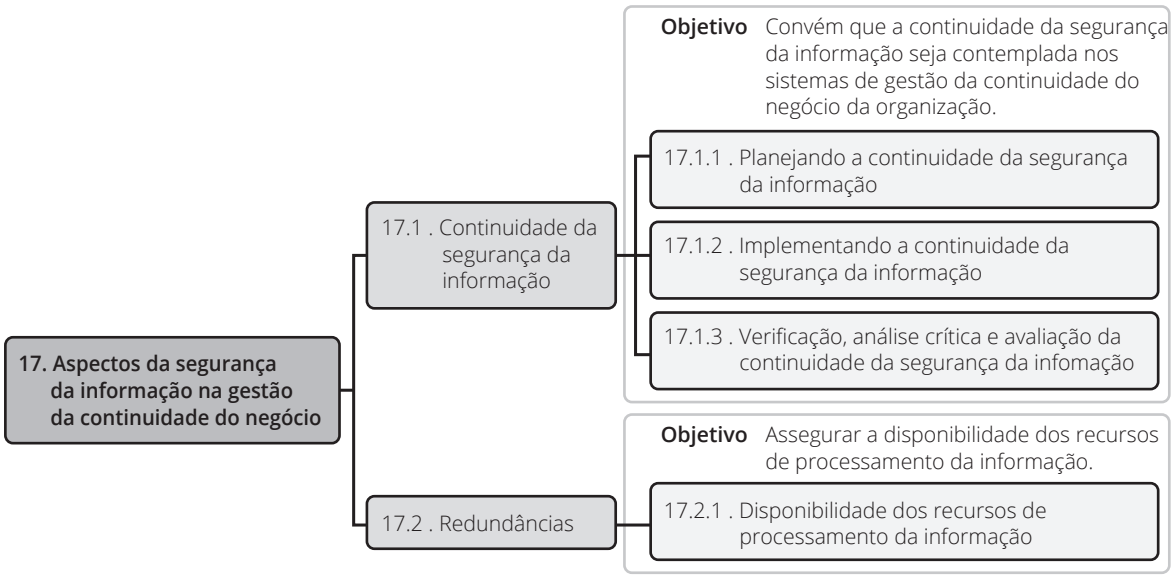


Figura 2.22
Seção 17, com suas duas categorias principais de segurança e seus controles.

A seção 17 (Aspectos da segurança da informação na gestão da continuidade do negócio) trata dos aspectos de continuidade no caso de ocorrência de um desastre. Essa seção possui duas categorias principais de segurança.

A categoria 17.1 (Continuidade da segurança da informação) tem por objetivo não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, além de assegurar a sua retomada em tempo hábil, se for o caso. Os controles são:

- **17.1.1 (Planejando a continuidade da segurança da informação**: convém que os requisitos para segurança da informação e a continuidade da gestão de segurança sejam determinados;
- **17.1.2 (Implementando a continuidade da segurança da informação)**: convém estabelecer, documentar, implementar e manter os processos, procedimentos e controles para assegurar a continuidade para a segurança da informação;
- **17.1.3 (Verificação, análise crítica e avaliação da continuidade da segurança da informação)**: convém que os controles sejam verificados em intervalos regulares;

A categoria 17.2 (Redundâncias) tem por objetivo assegurar a disponibilidade dos recursos de processamento da informação. Possui um controle:

- **17.2.1 (Disponibilidade dos recursos de processamento da informação)**: apresenta a necessidade de que deve haver redundância suficiente para atender aos requisitos de disponibilidade.

Exercício de fixação 12

Seção 17 – Aspectos da segurança da informação na gestão da continuidade do negócio

Utilizando a norma, explique os controles:

17.1.2.

17.1.3.

Seção 18 – Conformidade

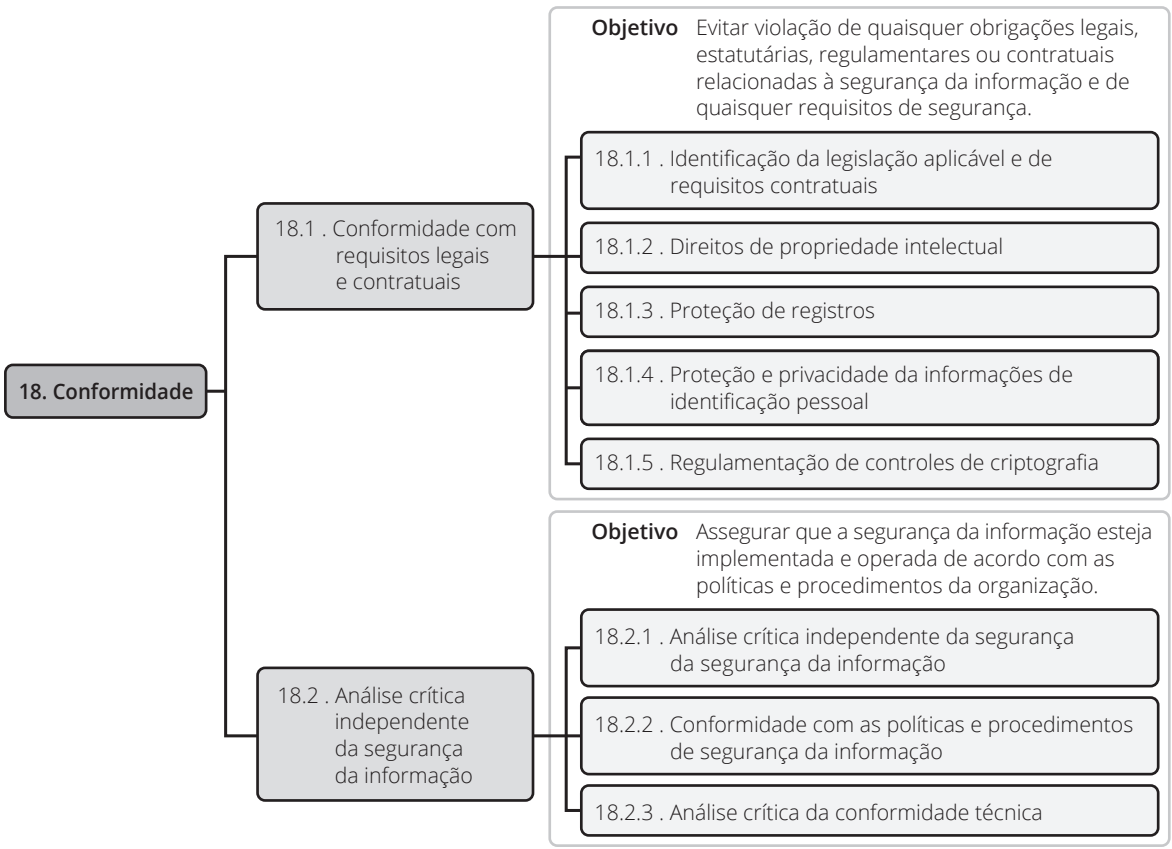


Figura 2.23 Seção 18, com suas duas categorias principais de segurança e seus controles.

A seção 18 (Conformidade) estabelece que os requisitos de segurança da informação estejam de acordo com qualquer legislação (legalidade), como regulamentações, estatutos ou obrigações contratuais. Essa seção possui três categorias principais de segurança.

A categoria 18.1 (Conformidade com requisitos legais e contratuais) tem por objetivo evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Possui os seguintes controles:

- **18.1.1 (Identificação da legislação aplicável e de requisitos contratuais)**: apresenta a conveniência de que todos os requisitos legais e contratuais sejam explicitamente definidos, documentados e mantidos;

- **18.1.2 (Direitos de propriedade intelectual)**: apresenta a conveniência de que procedimentos sejam implementados para garantir a conformidade em relação aos direitos de propriedade intelectual;
- **18.1.3 (Proteção de registros)**: apresenta a conveniência de que os registros sejam protegidos contra perda, destruição e falsificação;
- **18.1.4 (Proteção e privacidade de informações de identificação pessoal)**: apresenta a conveniência de que a privacidade e a proteção de dados sejam asseguradas;
- **18.1.5 (Regulamentação de controles de criptografia)**: convém que controles criptográficos sejam usados em conformidade com a legislação em vigor.

A categoria 18.2 (Análise crítica da segurança da informação) tem por objetivo garantir que a segurança da informação esteja implementada e operada de com as políticas e procedimentos. Seus controles são:

- **18.2.1 (Análise crítica independente da segurança da informação)**: apresenta a conveniência de que os gestores realizem em períodos regulares a análise crítica;
- **18.2.2 (Análise crítica da conformidade técnica)**: apresenta a conveniência de que os sistemas de informação sejam periodicamente verificados em sua conformidade.

Exercício de fixação 14
Seção 18 – Conformidade

Utilizando a norma, explique os controles:

18.1.1.

18.1.2.

18.1.4.

18.2.1.

18.3.1.

Roteiro de Atividades

Atividade 2.1 – Conhecendo a norma NBR ISO/IEC 27002:2013

1. Cite e justifique a categoria de controle de segurança da informação da norma NBR ISO/IEC 27002:2013, que trata da segurança física.

2. Ao analisar a documentação sobre segurança da informação da sua instituição, não foi identificada a existência de nenhuma política de segurança da informação. Cite e justifique a categoria de controle de segurança da informação da norma NBR ISO/IEC 27002:2013 que trata de política de segurança.

3. Como está estruturada cada categoria de controle?

Atividade 2.2 – Entendendo a norma NBR ISO/IEC 27002:2013

1. Qual o objetivo de controle da categoria 10.1 (Controles criptográficos)?

2. Descreva o controle 6.1.1 (Responsabilidades e Papeis pela segurança da informação).

3. Explique as diretrizes para a implementação do controle 11.2.9 (Política de mesa limpa e tela limpa).

4. Descreva as informações adicionais para 18.1.4 (Proteção e privacidade de informações de identificação pessoal).

Atividade 2.3 – Trabalhando com a norma NBR ISO/IEC 27002:2013

Em trabalho para a implementação de um sistema de gestão de segurança da informação, durante a realização da análise de risco, foram identificadas diversas vulnerabilidades, apresentadas no quadro a seguir. De posse da NBR ISO/IEC 27002:2013, indique o controle ou os controles dessa norma que devem ser implementados para tratar cada uma dessas vulnerabilidades. A primeira vulnerabilidade é respondida como exemplo.

N° ordem	Vulnerabilidade	Controle(s) n°(s)
01	Proteção física (porta) de acesso à sala dos servidores inadequada.	11.1.2
02	Rede elétrica instável.	
03	Controle de recrutamento inadequado de mão de obra.	
04	Falta de conscientização de segurança.	
05	Armazenamento inadequado do backup.	
06	Inexistência de controle de mudanças no desenvolvimento de software.	
07	Transferência de chaves e senhas em texto puro.	

Nº ordem	Vulnerabilidade	Controle(s) nº(s)
08	Documentos armazenados em local desprotegido.	
09	Documentos classificados deixados expostos sobre a mesa.	
10	Falta de proteção contra vírus e códigos maliciosos.	
11	Uso de dados de produção para testes de software em desenvolvimento.	
12	Controle inadequado/inexistente para realização de trabalho remoto.	
13	Controle inadequado de serviços terceirizados.	
14	Falta de procedimento para remoção de equipamentos para manutenção.	
15	Falta plano de testes dos planos de continuidade.	
16	Funcionário utilizando recursos computacionais para uso pessoal (download de filmes e músicas).	
17	Mesma senha utilizada por vários usuários.	
18	Não foram identificados sistemas ou procedimentos para entrada física em áreas seguras.	
19	Não existe um procedimento de classificação das informações.	
20	O funcionário que controla os servidores de aplicação desconhecia o procedimento em caso de eventos de segurança.	

Atividade 2.4 – Estudo de caso: sua organização

Considerando as respostas dadas para sua organização no estudo de caso do Roteiro de Atividades anterior, analise a situação da organização de acordo com as seções da norma e responda:

1. Quais seções da norma já estão plenamente implementadas na sua organização? Quais estão parcialmente? Justifique.

2. Quais seções são extremamente necessárias de acordo com os negócios da sua organização? Justifique.

3. Como você justificaria a necessidade de uso da norma e implementação dos seus controles? Justifique.

3

Sistema de Gestão da Segurança da Informação

objetivos

Apresentar uma visão geral e escopo do Sistema de Gestão da Segurança da Informação (SGSI), assim como uma análise crítica e detalhamento dos controles.

conceitos

Modelos SGSI.

Visão geral e escopo

O Modelo de Sistema de Gestão de Segurança da Informação (SGSI) integra a estratégia da organização, sendo influenciado por fatores como:

- Necessidades e objetivos.
- Requisitos de segurança.
- Processos.
- Estrutura organizacional.

A norma ABNT NBR ISO/IEC 27001:2013 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

Exercício de nivelamento 1
SGSI

O que você entende por gestão?

O que você entende por sistema de gestão?

A adoção de um SGSI deve ser uma decisão estratégica para a organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização.

É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização; por exemplo, uma situação simples requer uma solução de um SGSI simples.

Modelo PDCA

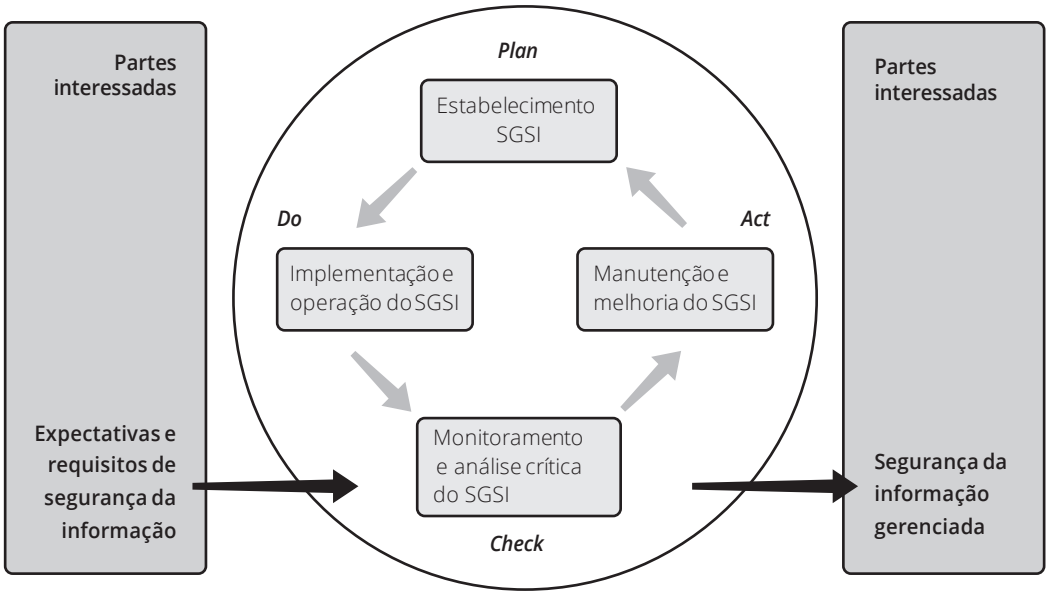


Figura 3.1
Modelo PDCA.

A norma ISO 27001 adota o modelo conhecido como "Plan-Do-Check-Act" (PDCA), que é aplicado para estruturar todos os processos do Sistema de Gestão da Segurança da Informação (SGSI).

O modelo PDCA compõe um conjunto de ações em sequência estabelecida pelas letras que compõem a sigla: P (plan: planejar), D (do: fazer, executar), C (check: verificar, controlar) e finalmente o A (act: agir, atuar corretivamente):

- **Plan** (planejar: estabelecer o SGSI): estabelecer a política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e melhoria da segurança da informação, para produzir resultados de acordo com as políticas e objetivos globais de uma organização;
- **Do** (fazer: implementar e operar o SGSI): implementar e operar a política, controles, processos e procedimentos do SGSI;
- **Check** (checar: monitorar e analisar criticamente o SGSI): avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção;
- **Act** (agir: manter e melhorar o SGSI): executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e na análise crítica realizada pela direção ou em outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Saiba mais

A norma ABNT NBR ISO/IEC 27003:2011 – Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação – apresenta de forma detalhada os aspectos críticos necessários para a implantação e projetos bem-sucedidos de um Sistema de Gestão da Segurança da Informação (SGSI), de acordo com a ABNT NBR ISO IEC 27001:2005. A norma descreve o processo de especificação e projeto do SGSI desde a concepção até a elaboração dos planos de implantação. A norma descreve o processo de obter a aprovação da direção para implementar o SGSI, define um projeto para implementar um SGSI (referenciado nesta Norma como o projeto SGSI), e fornece diretrizes sobre como planejar o projeto do SGSI, resultando em um plano final para implantação do projeto do SGSI.

Exercício de fixação 1
Modelo PDCA

Explique o modelo PDCA.

Explique como o modelo PDCA pode ser aplicado ao SGSI.

Sistema de Gestão da Segurança da Informação (SGSI)

Requisitos gerais:

- A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI.

Estabelecendo e gerenciando o SGSI.

Requisitos da documentação.

O Sistema de Gestão da Segurança da Informação (SGSI), em inglês Information Security Management System (ISMS), é um processo estruturado de tratamento da segurança da informação nos diversos setores. Veremos agora seus principais pontos, para uma perfeita implementação.

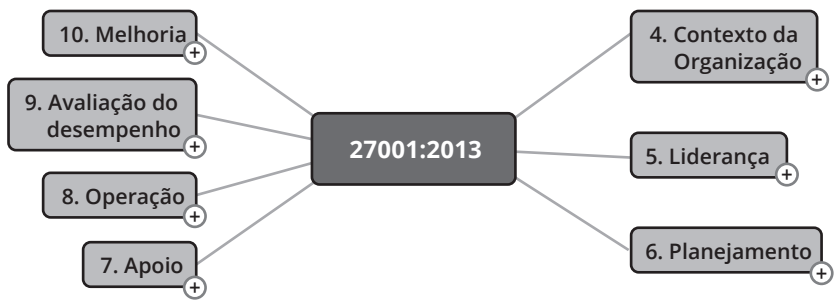


Figura 3.2
Visão da estrutura da Norma NBR ISO/IEC 27001:2013.

A norma NBR ISO/IEC 27001:2013 está estruturada em dez sessões e um anexo. As sessões de 1 a 3 tratam do escopo, da referência normativa e termos e definições. As demais sessões a partir da 4 buscam de forma objetiva e genérica apresentar os requisitos aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.

Vejamos a seguir cada fase da gestão de um Sistema de Gestão da Segurança da Informação (SGSI):

- 4. Contexto da organização;
- 5. Liderança;
- 6. Planejamento;
- 7. Apoio;
- 8. Operação;
- 9. Avaliação do desempenho;
- 10. Melhoria;
- Anexo A.

Contexto da Organização

- Entendendo a organização e seu contexto.
- Entendendo as necessidades e as expectativas das partes interessadas.
- Determinar o escopo do sistema de gestão da segurança da informação.
- Sistema de gestão da segurança da informação.

Este capítulo aborda a necessidade de entender todo o contexto da organização, ou seja, interpretar ou analisar toda a organização para determinar as questões internas e externas que possam afetar a capacidade do sistema de gestão da segurança da informação.

De acordo com a ABNT NBR ISO/IEC 27003:2011 – Tecnologia da Informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação, normalmente, para iniciar o projeto do SGSI, é necessária a aprovação da direção da organização. Para isso, é importante que a primeira atividade a ser desempenhada seja coletar informações relevantes que demonstrem o valor de um SGSI para a organização, esclarecendo por que é necessária a implantação de um SGSI.

É importante que a organização determine as partes interessadas importantes para o sistema de da segurança da informação e os requisitos que essas partes interessadas demandam de segurança da informação.

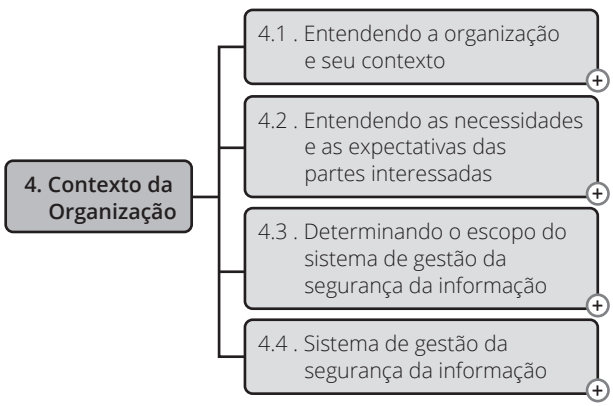


Figura 3.3
Etapas da seção 4 – Contexto da Organização da norma ABNT NBR ISO/IEC 27001:2013.

Na determinação do escopo, a organização deve considerar as questões internas e externas, os requisitos e as interfaces, e dependências entre as atividades desempenhadas pela organização. As seguintes atividades são necessárias:

- Definir o escopo e os limites organizacionais;
- Escopo e limites da Tecnologia da Informação e Comunicação (TIC);
- Escopo e limites físicos;
- O negócio, a organização, sua localização, ativos e aspectos tecnológicos do escopo, políticas;

Liderança

- Liderança e comprometimento.
- Política.
- Autoridades, responsabilidades e papéis organizacionais.

5.2 Política de Segurança da Informação:

- Apropriada ao propósito.
- Incluir os objetivos de segurança da informação ou a estrutura para estabelecê-los.
- Incluir comprometimento em satisfazer os requisitos aplicáveis.
- Incluir comprometimento com a melhoria contínua.
- Deve:
  - Estar disponível.
  - Ser comunicada.
  - Estar disponível para as partes interessadas.

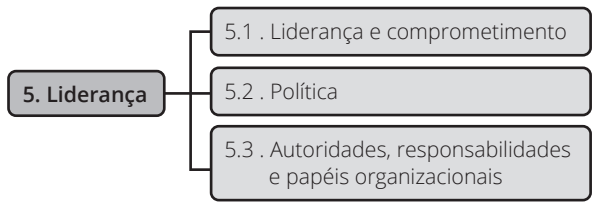


Figura 3.4
Etapas da seção 5 – Liderança da norma ABNT NBR ISO/IEC 27001:2013.

A norma destaca a importância, para o sucesso do SGSI, do requisito liderança. O envolvimento da Alta Direção, através da sua liderança e comprometimento, devem ser demonstrados durante todo o processo do SGSI.

Essa liderança inicia-se pelo estabelecimento da política de segurança e os objetivos de segurança da informação compatíveis com a direção estratégica da organização. A política deve ser formalizada e comunicada, e ainda ser apropriada ao propósito da organização, entre outros.

Leia a seção 5 da norma ABNT NBR ISO/IEC 27001:2013.

Exercício de fixação 2
Liderança

Explique o requisito de definir política de segurança no estabelecimento de um SGSI. Use a norma 27001.

Planejamento

- 6.1 Ações para contemplar riscos e oportunidades.
  - Geral.
  - Avaliação de riscos de segurança da informação.
  - Tratamento de riscos de segurança da informação.
- 6.2 Objetivo de segurança da informação e planejamento para alcançá-los.

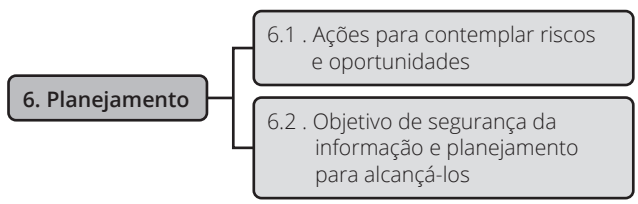


Figura 3.5
Etapas da seção 6 Planejamento da norma ABNT NBR ISO/IEC 27001:2013.

A seção 6 aborda as etapas de planejamento de um SGSI que incluem definir e aplicar um processo de avaliação de riscos de segurança da informação. Todo esse processo deve ser documentado e retido. Todo o processo de avaliação e tratamento dos riscos dever estar alinhado com os princípios e diretrizes das normas ABNT NBR ISO 31000 e ABNT NBR ISO 27005.

A norma ABNT NBR ISO/IEC 27003:2011 – Tecnologia da Informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação – cita em suas diretrizes para implementação que a avaliação da segurança da informação é a atividade para identificar o nível existente de segurança da informação (ou seja, os atuais procedimentos organizacionais de tratamento da proteção da informação). O objetivo fundamental da avaliação de segurança da informação é fornecer informações de apoio necessárias para a descrição do sistema de gestão sob a forma de políticas e diretrizes.

O desempenho de uma análise/avaliação de riscos de segurança dentro do contexto de negócios apoiado pelo escopo do SGSI é essencial para a conformidade e a implementação bem-sucedida do SGSI, de acordo com a ABNT NBR ISO/IEC 27001:2013.

Leia a seção 6 da norma ABNT NBR ISO/IEC 27001:2013.

Exercício de fixação 3
Planejamento

Cite dois objetivos de segurança da informação.

Apoio

- Recursos.
- Competência.
- Conscientização.
- Comunicação.
- Informação documentada.
  - Geral.
  - Criando e atualizando.
  - Controle da informação documentada.

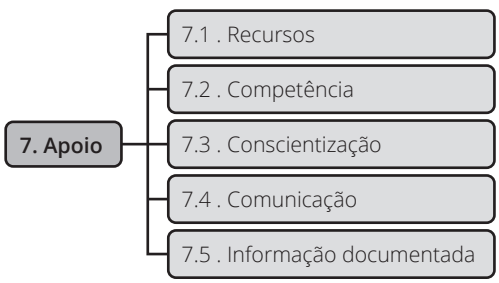


Figura 3.6
Etapas da seção 7 Apoio da norma ABNT NBR ISO/IEC 27001:2013.

Essa seção trata dos recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI.

Outro aspecto tratado é sobre a definição das competências necessária das pessoas. O Anexo B (informativo) Papéis e responsabilidades pela Segurança da Informação, da norma ABNT NBR ISO/IEC 27003:2011 – Tecnologia da Informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação, apresenta a tabela a seguir com uma lista exemplificada de papéis e responsabilidades pela segurança informação:

Papel	Breve descrição da responsabilidade
Alta administração (exemplo: COO, CEO, CSO e CFO).	É o responsável pela visão, decisões estratégicas e pela coordenação de atividades para dirigir e controlar a organização.
Gerentes de linha (isto é, o último nível de comando na escala hierárquica	Tem a responsabilidade final pelas funções organizacionais.
Diretor-executivo de Segurança da Informação.	Tem a responsabilidade e a governança globais em relação à segurança da informação, garantindo o correto tratamento dos ativos de informação.
Comitê de Segurança da Informação (membro do comitê).	É responsável por tratar ativos de informação e tem um papel de liderança no SGSI da organização.
Equipe de Planejamento da Segurança da Informação (membro da equipe).	É responsável durante as operações, enquanto o SGSI está sendo implantado. A Equipe de Planejamento trabalha em diversos departamentos e resolve conflitos até que a implantação do SGSI seja concluída.
Parte interessada.	No contexto das outras descrições de papéis relativos à segurança da informação, a parte interessada é aqui definida primariamente como pessoas e/ou órgãos que estão fora das operações normais – como o conselho e os proprietários (tanto proprietários da organização, se esta for parte de um grupo de empresas ou se for governamental, quanto proprietários diretos, como acionistas de uma organização privada). Outros exemplos de partes interessadas podem ser companhias associadas, clientes, fornecedores e demais organizações públicas, como agências governamentais de regulação financeira ou bolsa de valores, se a organização não estiver listada.
Administrador de sistema.	O administrador de sistema é responsável por um sistema de TI.
Gerente de TI.	É o gerente de todos os recursos de TI (por exemplo, o Gerente do Departamento de TI).
Segurança Física.	A pessoa responsável pela segurança física, por exemplo, construções etc., normalmente chamado de Gerente de instalações.
Gerência de Risco.	A(s) pessoa(s) responsável(eis) pela estrutura de gerenciamento de risco da organização, incluindo avaliação de risco, tratamento de risco e monitoramento de risco.
Consultor Jurídico.	Muitos riscos de segurança da informação têm aspectos legais, e o consultor jurídico é responsável por levar esses riscos em consideração.
Recursos Humanos.	É (São) a(s) pessoa(s) com responsabilidade global pelos funcionários.

Papel	Breve descrição da responsabilidade
Arquivo.	Todas as organizações têm arquivos contendo informações vitais e que precisam ser armazenadas por longo tempo. As informações podem estar localizadas em vários tipos de mídia, e convém que uma pessoa específica seja responsável pela segurança desse armazenamento.
Dados Pessoais.	Se for exigência legal, pode haver uma pessoa responsável por ser o contato com um conselho de inspeção de dados ou organização oficial similar que supervisione a integridade pessoal e questões de privacidade.
Desenvolvedor de Sistema.	Se uma organização desenvolve seus próprios sistemas de informação, alguém tem a responsabilidade por esse desenvolvimento.
Especialista/Expert.	Convém que seja feita referência a especialistas e experts, responsáveis por determinadas operações em uma organização quanto ao interesse destes nos assuntos pertinentes ao uso do SGSI nas suas áreas específicas de atuação.
Consultor Externo.	Consultores externos podem emitir opiniões com base em seus pontos de vista macroscópicos da organização e em suas experiências na indústria. Contudo, pode ser que os consultores não tenham conhecimento aprofundado da organização e suas operações.
Empregado/Funcionário/ Usuário.	Cada empregado é igualmente responsável pela manutenção da segurança da informação no seu local de trabalho e em seu ambiente.
Auditor.	O auditor é responsável por avaliar o SGSI.
Instrutor.	O instrutor ministra treinamentos e executa programas de conscientização.
Responsável pela TI ou pelos Sistemas de Informação (SI) locais.	Em uma organização maior, há geralmente alguém na organização local que é responsável pelos assuntos de TI, e provavelmente também pela segurança da informação.
Defensor (pessoa influente).	Esse não é, em si, um papel de responsabilidade propriamente dito, mas, em uma organização maior, pode ser muito útil durante o estágio de implementação contar com pessoas que tenham conhecimento aprofundado sobre a implementação do SGSI e que possam apoiar o entendimento sobre a implementação e as razões que estiverem por trás dela. Essas pessoas podem influenciar positivamente a opinião das outras e podem também ser chamadas de "Embaixadoras".

Tabela 3.1
Lista exemplificada de papéis e responsabilidades pela segurança da informação. Anexo B da norma ABNT NBR ISO/IEC 27003:2011 – Diretrizes para implantação de um sistema de gestão da segurança da informação.

A comunicação e as atividades de conscientização são etapas importantes para o sucesso de um SGSI. A organização deve implementar um programa de conscientização, treinamento e educação em segurança da informação para que toda a organização entenda seus papéis e suas competências para executarem as operações necessárias ao SGSI.

A documentação dentro de um SGSI é um importante fator de sucesso, pois demonstrará a relação dos controles implementados com os resultados esperados. A documentação muitas vezes será a evidência necessária para averiguar que um SGSI está implementado de forma correta e eficiente, permitindo que as ações possam ser rastreáveis e passíveis de reprodução.

Saiba mais

Declaração de aplicabilidade é um documento formal contendo os controles aplicados, os controles não aplicados, os controles não aplicáveis e os controles adicionais. É uma listagem de todos os controles da norma assinalando: os controles aplicados e riscos que estão sendo tratados; os controles não aplicados e as justificativas da sua não aplicação; e os controles não aplicáveis no ambiente da organização com suas justificativas.

Os documentos listados a seguir são requisitos gerais e a base documental para que possa ser realizada a auditoria de um SGSI:

1. Declaração da política de segurança e objetivos do SGSI;
2. Escopo;
3. Procedimentos e controles;
4. Descrição da metodologia de análise/avaliação de riscos;
5. Relatório de análise/avaliação de riscos;
6. Plano de tratamento de riscos;
7. Procedimentos necessários para garantia da efetividade, operação e controles;
8. Descrição da medição da efetividade dos controles;
9. Registros requeridos.

- Declaração da política de segurança e objetivos do SGSI.
- Escopo.
- Procedimentos e controles.
- Descrição da metodologia de análise/avaliação de riscos.
- Relatório de análise/avaliação de riscos.
- Plano de tratamento de riscos.
- Procedimentos necessários para garantia da efetividade, operação e controles.
- Descrição da medição da efetividade dos controles.
- Registros requeridos.
- Declaração de aplicabilidade.

Leia a seção 7 da norma ABNT NBR ISO/IEC 27001:2013.

Exercício de fixação 4
Apoio

Por que essa fase é importante? Use a norma 27001 para responder.

Operação

- Planejamento operacional e controle.
- Avaliação de riscos de segurança da informação.
- Tratamento de riscos de segurança da informação.

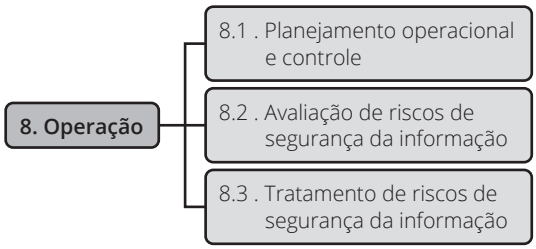


Figura 3.7
Etapas da seção 8 – Operação da norma ABNT NBR ISO/IEC 27001:2013.

Na seção 8 a norma trata das atividades ligadas a operação do SGSI. Nesta etapa a organização planeja todos os passos necessários para atender os requisitos de segurança da informação e implementar as ações necessárias. A organização deve manter tudo documentado, processos e mudanças, para que possa gerar confiança de que tudo esta seguindo o planejado.

A organização deve ainda implementar uma metodologia para realizar avaliações de risco e, a partir da sua aplicação, implementar um plano de tratamento nos riscos identificados.

Leia a seção 8 da norma ABNT NBR ISO/IEC 27001:2013.

Avaliação do desempenho

- Monitoramento, medição, análise e avaliação.
- Auditoria interna.
- Análise crítica pela Direção.

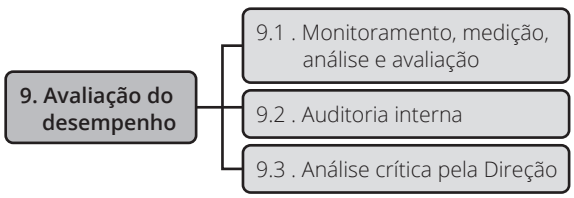


Figura 3.8
Etapas da seção 9 – Avaliação do desempenho da norma ABNT NBR ISO/IEC 27001:2013.

Nesta seção, de avaliação do desempenho, a norma destaca a importância do monitoramento para verificar a eficácia do SGSI, através da determinação do que deve ser monitorado e medido.

Figura 3.9
Fluxo do processo de Monitoramento segundo a norma ABNT NBR ISO/IEC 27003 – Diretrizes para implantação de um sistema de gestão da segurança da informação.

A implantação do SGSI deve ser avaliada em intervalos regulares por meio de auditorias internas e independentes. Essas auditorias servirão para conferir e avaliar as experiências obtidas na prática, do dia a dia.

Uma auditoria deve ser planejada levando em consideração o status e a importância dos processos e áreas a serem auditadas, bem como o resultado das auditorias anteriores.

Leia a seção 9 da norma ABNT NBR ISO/IEC 27001:2013.

Devem ser definidos critérios de auditoria, abrangência, frequência e método.

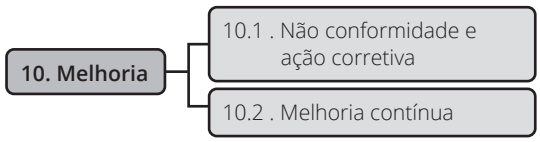
Essenciais em qualquer sistema de gestão, as atividades de monitoração e análise crítica são fundamentais para o sucesso de um SGSI, por permitirem o acompanhamento, através de evidências, e também o processo de melhoria contínua do sistema.

A análise crítica pela Direção deve analisar criticamente o SGSI em intervalos regulares planejados, para assegurar a sua contínua adequação, pertinência e eficácia aos objetivos estratégicos da organização.

Melhoria

- Não conformidade e ação corretiva.
- Melhoria contínua.

Figura 3.10 Etapas da seção 10 – Melhoria da norma ABNT NBR ISO/IEC 27001:2013.



A seção 10 aborda os aspectos de melhoria e aperfeiçoamento do SGSI, quando uma não conformidade ocorre, a fim de que a organização possa tomar as ações necessárias para controlar e corrigir.

Não conformidade
É o não atendimento a um requisito; é um fato que contraria um requisito, sendo comprovado por evidências. Em determinados casos, a falta de evidência é uma evidência. Não Conformidade Maior: é quando um requisito inteiro da norma não é atendido, caracterizando uma falha sistêmica. Também poderão acontecer quando falhas existirem nos produtos e for constatado que os clientes estão recebendo produtos com falhas. Caracteriza também o acúmulo de não conformidades menores a um mesmo item normativo ou então a reincidência de uma não conformidade menor identificada em uma auditoria externa anterior. Não Conformidade Menor: lapso do controle de um requisito pré-estabelecido; apesar de não ser grave, indica não cumprimento de um processo específico.

Essa fase busca apresentar os requisitos que a organização, de forma regular e estruturada, deve atender para que o seu SGSI mantenha-se dentro do processo de melhoria contínua do PDCA.

A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança, resultados de auditoria, análise de eventos monitorados, ações corretivas e preventivas e revisão da direção.

- **Ações corretivas**: a organização deve tomar ações corretivas para eliminar as causas das **não conformidades** com os requisitos do SGSI, para evitar a sua repetição;
- **Ações preventivas**: a organização deve determinar ações para eliminar as causas de não conformidades potenciais com os requisitos da SGSI, para evitar a sua ocorrência.

A melhoria contínua deve ser um processo implantado na organização buscando o constante aperfeiçoamento e melhoria de todo o sistema de gestão da segurança da informação.

Anexo A

- Controles e objetivos de controle.
- Alinhados com a ABNT NBR ISO/IEC 27002:2013 (Seções 5 a 18).
- Devem ser usados com 6.1.3 – Tratamento de riscos de segurança da informação.

O Anexo A da norma ABNT NBR ISO/IEC 27001:2013 lista os controles que, de acordo com a norma, devem ser implementados na implementação de um SGSI. Os controles são semelhantes aos existentes na ABNT NBR ISO/IEC 27002:2013, com a diferença de que contém o verbo “dever”, que apresenta circunstâncias que são externas ao participante envolvido numa situação de segurança , mas que a tornam necessária, com um sentido de “dever”, “ter de”. Assim, os controlem “devem” ser implementados para que seja possível que se tenha um SGSI.

Porém, pode haver o caso de que nem todos os controles listados podem ou necessitam ser implementados. Nesse caso, a organização, ao criar um documento chamado "Declaração de Aplicabilidade", deve fazer constar os controles não implementados e os motivos da não aplicação.

No anexo A, o número do controle é antecedido pela letra "A". Assim, quando se refere a um controle do Anexo A da norma 27001:2013, este deve ser feito da seguinte forma: A.xx.xx.xx. No caso da norma 27002:2013, a referência tem apenas os números: xx.xx.xx.

Apesar de os controles serem semelhantes, o anexo A da norma 27001:2013 é usado para a implementação de controles dentro de um ambiente de SGSI, enquanto os controles da norma 27002:2013 são um código de boas práticas de segurança da informação.

Leia o Anexo A da norma ABNT NBR ISO/IEC 27001:2013.

Lista de verificação para implantação de um SGSI

A seguir é apresentada, como sugestão, uma lista de verificação para implantação de um SGSI, criada com base nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27003:2011:

Tabela 3.2
Exemplo de uma lista de verificação para implantação de um SGSI.

	Atividade	Resultado
01	Identificar os objetivos de negócio da organização.	▫ Lista de objetivos de negócio corporativo.
02	Conhecer os sistemas de gestão existentes na organização.	▫ Descrição dos sistemas de gestão existentes.
03	Definir objetivos, necessidades de segurança da informação e requisitos de negócio para o SGSI.	▫ Resumo dos objetivos, das necessidades de segurança da informação e dos requisitos de negócio para o SGSI.
04	Reunir normas regulamentares, de conformidade e do setor pertinentes à organização.	▫ Resumo das normas regulamentares, de conformidade e do setor pertinentes à organização.
05	Definir escopo preliminar do SGSI.	▫ Descrição do escopo preliminar do SGSI. ▫ Definição dos papéis e responsabilidades do SGSI.
06	Criar o plano de negócio e o plano de projeto para aprovação da direção.	▫ Plano de negócio e plano de projeto proposto.
07	Obter aprovação e comprometimento da direção para iniciar o projeto da implementação do SGSI.	▫ Aprovação da direção para iniciar o projeto da implementação do SGSI.
08	Definir os limites organizacionais.	▫ Descrição dos limites organizacionais. ▫ Funções e estrutura da organização. ▫ Troca de informações através dos limites. ▫ Processos de negócio e as responsabilidades pelos ativos da informação de dentro e de fora do escopo.
09	Definir limites de tecnologia da informação e comunicação.	▫ Descrição dos limites do TIC. ▫ Descrição dos sistemas de informação e redes de telecomunicações, detalhando o que está dentro e o que está fora do escopo.
10	Definir os limites físicos.	▫ Descrição dos limites físicos do SGSI. ▫ Descrição da organização e de suas características geográficas, detalhando o escopo interno e o externo.

	Atividade	Resultado
11	Finalizar os limites para o escopo do SGSI.	▫ Documento descrevendo o escopo e os limites do SGSI.
12	Desenvolver a política do SGSI.	▫ Política do SGSI aprovada pela direção.
13	Definir os requisitos de segurança da informação que apoiam o SGSI.	▫ Lista dos principais processos, funções, locais, sistemas de informação e redes de comunicação. ▫ Requisitos da organização sobre confidencialidade, disponibilidade, integridade e autenticidade. ▫ Requisitos da organização contemplando requisitos de segurança da informação legais, regulamentares, contratuais e do negócio.
14	Ativos identificados dentro do escopo do SGSI.	▫ Descrição dos principais processos da organização. ▫ Identificação dos ativos de informação dos principais processos da organização. ▫ Classificação dos processos e ativos críticos.
15	Conduzir a análise/avaliação de segurança da informação.	▫ Documento da avaliação e da descrição do status real da segurança da informação, incluindo controles de segurança da informação existentes (qual o real status da segurança da informação na organização?). ▫ Documento de deficiência da organização analisadas e avaliadas (quais os problemas? Que soluções são possíveis?).
16	Conduzir uma avaliação de risco.	▫ Escopo para a análise/avaliação de riscos (dentro do escopo do SGSI). ▫ Metodologia de análise/avaliação de riscos aprovada e alinhada com o contexto de gestão estratégica de riscos da organização (vide ABNT NBR ISO/IEC 31000 e ABNT NBR ISO/IEC 27005). ▫ Critérios de aceitação de riscos.
17	Selecionar os objetivos de controle e os controles.	▫ Análise/avaliação de alto nível de riscos documentada. ▫ Identificar a necessidade de uma análise/avaliação de riscos mais detalhada. ▫ Análise/avaliação de riscos detalhada e documentada. ▫ Resultados agregados da análise/avaliação de riscos.
18	Obter aprovação da direção para implementar o SGSI.	▫ Riscos e suas opções de tratamento identificadas. ▫ Objetivos de controle e controles selecionados para redução do risco.
19	Aprovação da direção para os riscos residuais.	▫ Aprovação documentada da direção para os riscos residuais propostos (convém que seja a saída da atividade anterior).
20	Autorização da direção para implementar e operar o SGSI.	▫ Autorização documentada da direção para implementar e operar o SGSI.
21	Preparar a Declaração de Aplicabilidade.	▫ Declaração de Aplicabilidade.
22	Definir a segurança organizacional.	▫ Estrutura da organização e seus papéis e responsabilidades relacionados à segurança da informação. ▫ Identificação de documentação relacionada ao SGSI. ▫ Modelos de registros do SGSI e instruções de uso e armazenamento. ▫ Documento de política de segurança da informação. ▫ Linha de base de políticas e procedimentos de segurança da informação (e, se aplicável, planos para desenvolver políticas, procedimentos específicos, entre outros).

	Atividade	Resultado
23	Projetar a segurança física e de TIC.	▫ Planos de projeto de implementação para o processo de implementação dos controles de segurança selecionados para a segurança física e de TIC .
24	Definir a segurança da informação específica para o SGSI.	▫ Procedimentos descrevendo os processos de comunicação de informações e de analise crítica pela direção.
25	Definir a auditoria e monitoramento.	▫ Descrições para auditoria, monitoramento e medição.
26	Definir um programa de conscientização.	▫ Detalhar um programa de treinamento e conscientização.
27	Produzir o plano de projeto final do SGSI.	▫ Plano de projeto de implementação para os processos de implementação aprovados pela direção.
28	Plano de projeto final do SGSI.	▫ Um plano de projeto de implementação do SGSI específico para a organização, abrangendo a execução de atividades planejadas para a segurança da informação física, de TIC e organizacional, bem como os requisitos específicos do SGSI para implementá-lo de acordo com os resultados das atividades abrangidas pelas normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27003.

Roteiro de Atividades 3

Atividade 3.1 – Conhecendo o ciclo PDCA

Descreva as principais atividades de um SGSI em cada etapa do ciclo PDCA (Plan-Do-Check-Act).

Atividade 3.2 – Contexto da organização

Relacione os requisitos que, segundo a norma, devem constar obrigatoriamente no estabelecimento do contexto da organizaçãode um SGSI (Sistema de Gestão de Segurança da Informação).

Atividade 3.3 – Planejamento

Quais são as ações para contemplar riscos e oportunidades?

Quais os objetivos de segurança da informação para a sua organização? Justifique sua resposta.

Atividade 3.4 – Apoio

Qual a importância da conscientização e comunicação?

Atividade 3.5 – Documentos

Quais são os documentos que devem ser incluídos no SGSI?

O que é a Declaração de Aplicabilidade?

Atividade 3.6 – Operação

Considerando o atual status da segurança da informação na sua instituição, apresente as etapas da Operação mínimas e necessárias para que a implementação do SGSI ocorra num prazo de até um ano. Indique os prazos a serem considerados em cada etapa.

De acordo com a sua resposta anterior, cite sequencialmente os documentos necessários para essa implementação.

4

Política de segurança da informação

objetivos

Identificar os requisitos, construir e usar uma política de segurança da informação.

conceitos

Política de segurança, normas, procedimentos e boas práticas.

Definição

- Conjunto de regras gerais que direcionam a segurança da informação e são suportadas por normas e procedimentos.
- Devem ser seguidas por toda a organização, orientando a segurança da informação, conforme o ramo de negócio, legislação e normas vigentes.
- A política de segurança deve ser clara e objetiva.
- E pode ser considerada um documento jurídico.

Inicialmente, serão vistos os seguintes tópicos referentes à política de segurança: definição, escopo e algumas questões relevantes a considerar, com vistas ao seu desenvolvimento e à sua implantação nas organizações.

Exercício de nivelamento 1
Política de segurança da informação

O que você entende por política?

Na sua opinião, como deve ser uma política de segurança?

A política de segurança da informação é um conjunto de diretrizes apoiado por normas e procedimentos, que determinam as regras e práticas a serem seguidas para assegurar a segurança da informação, de acordo com o ramo de negócio e requisitos legais, contratuais, regulamentares e normativos aplicáveis a todo o escopo da organização. Ela definirá as diretrizes, os limites, as responsabilidades e os objetivos dos controles que deverão ser implementados e implantados para garantir os requisitos de proteção da segurança da informação na organização.

Sendo assim, a política de segurança deve ser claramente definida, publicada e mantida atualizada e apoiada pelos dirigentes da organização.

A importância da política de segurança para o SGSI é alta, uma vez que representa um documento formal, até mesmo com valor jurídico.

Saiba mais

Antes de iniciar este capítulo, faça uma leitura completa da Seção 5 – Políticas de Segurança da Informação, da norma ABNT NBR ISO/IEC 27002:2013.

Diagrama

Figura 4.1
Sequência e relação da política de segurança com fases do planejamento.

Políticas	Diretrizes que devem ser seguidas. Responde ao "porquê" de realizar a Segurança da Informação, definindo diretrizes genéricas do que deve ser realizado pela organização para alcançar a Segurança da informação.
Normas	Regras básicas de como deve ser implementado o controle ou conjunto de controles, que foram definidos nas políticas. Respondem "o quê" fazer para se alcançar as diretrizes definidas na política de segurança.
Procedimentos	Atividades detalhadas de como deve ser implementado o controle ou conjunto de controles. Respondem "como" fazer cada item definido nas normas específicas e suas políticas.
Instruções	Descrição de uma operação ou conjunto de operações para a execução da implementação de controles de segurança da informação.
Evidências	Mecanismos adotados para permitir a coleta e comprovação da aplicação dos controles de segurança da informação, sua eficácia e eficiência. Permitirá a rastreabilidade e uso em auditorias.

Tabela 4.1
A Política de segurança da informação em detalhes.

A política de segurança de uma organização é composta por diretrizes gerais que servirão de base para as normas, procedimentos e instruções referentes à segurança da informação.

Devem estar alinhadas com a norma ABNT ISO 27001, com a legislação vigente e com as normas gerais pelas quais a organização se orienta.

Exercício de fixação 1
Diagrama

Quais são os procedimentos formalizados existentes na área de TI da sua organização?

Arquitetura das políticas de segurança

Não existe uma arquitetura padrão para a definição das políticas de segurança. Elas devem seguir e atender aos requisitos de negócios da organização e sua cultura organizacional. Para uma boa estruturação das políticas de segurança, podemos ter por base as dimensões da segurança da informação apresentadas no livro *Praticando a Segurança da Informação*:

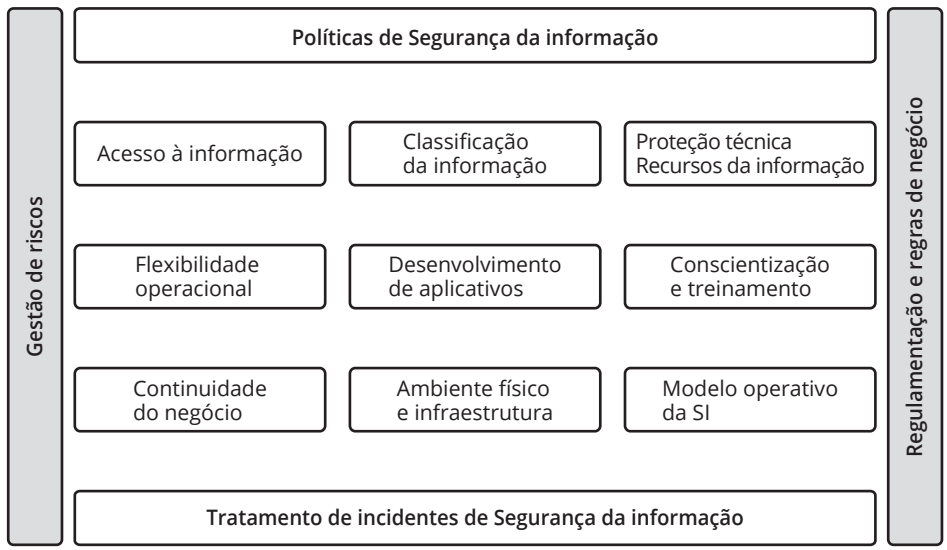


Figura 4.2
Estrutura baseada na Norma Internacional ISO/IEC 27002:2013.

Estas podem ser vistas como as políticas de segurança necessárias, mas que devem ser adequadas às necessidades de cada organização. É de suma importância que cada organização estabeleça a arquitetura que precisa ter para atender aos seus requisitos de segurança e de negócios.

Escopo

- Estabelece princípios para a proteção, o controle e o monitoramento de recursos e informações.
- Estabelece as responsabilidades da segurança da informação.

Em uma organização, a política de segurança deve:

- Estabelecer os princípios a serem seguidos com o intuito de proteger, controlar e monitorar seus recursos e sua informação;
- Em especial, a política de segurança da informação pode ser integrada a outras políticas e planos vigentes na organização, tais como políticas de contingência e plano estratégico de negócios.
- Ao definir o escopo da política, detalhar os limites de aplicação dela, citando os ambientes, físicos, lógicos e organizacionais que são aplicáveis e tipos de usuários, entre outros.

Exercício de fixação 2
Escopo

Qual o detalhamento necessário para definir o escopo da política de segurança da sua organização?

Questionamentos importantes

- O que se quer proteger?
- Contra o quê ou quem?
- Quais são as ameaças mais prováveis?
- Qual a relevância de cada recurso?
- Qual o grau de proteção requerido?
- Quanto tempo, recursos financeiros e humanos se pretende gastar?
- Quais as expectativas dos usuários e clientes?

Com o objetivo de definir uma política de segurança da informação para uma organização, deve-se ter em mente as respostas às seguintes questões:

- O que se quer proteger? Ativos da organização necessitam de proteção.
- Contra o quê ou quem? Quais são as ameaças que podem afetar a organização e de que forma e por quem estas ameaças podem ser exploradas?
- Quais são as ameaças mais prováveis? Identificar dentre as ameaças as que possuem maior probabilidade de ocorrer.
- Qual a relevância de cada recurso a ser protegido? Importância do recurso dentro do processo de negócio.
- Qual o grau de proteção requisitado? Requisitos de proteção que o negócio exige. Qual nível de proteção é necessário?
- Quanto tempo, recursos financeiros e humanos serão disponibilizados? Quais recursos estão disponíveis para os objetivos de segurança? O que pode ser feito com os recursos existentes?
- Quais as expectativas dos usuários e clientes? O que esperam da segurança da informação para o negócio da organização, serviços e produtos?

Com isso, podem ser aplicados mecanismos de segurança adequados aos requisitos de segurança indicados na política. Em adição, com as devidas respostas em mente, pode-se analisar os riscos e requisitos legais e de normas, de acordo com a política de segurança.

Etapas

- Identificar a legislação.
- Identificar recursos críticos.
- Analisar necessidades de segurança.
- Elaborar proposta e promover discussão aberta.
- Apresentar documento.
- Aprovar e implementar.
- Comunicar e treinar.
- Manter a política de segurança.

A política de segurança deve ser implantada segundo um processo formal, embora flexível, de modo a permitir alterações de acordo com as necessidades. Uma proposta típica para a implantação de uma política de segurança da informação compreende:

- Identificar a legislação aplicável na organização;
- Identificar os recursos críticos;
- Classificar as informações da organização, observando não apenas a área de informática, mas todos os setores e suas respectivas informações;
- Analisar as necessidades de segurança, com o objetivo de verificar possíveis ameaças, riscos e impactos na organização;
- Elaborar a proposta para a política de segurança;
- Discutir abertamente com todos os envolvidos o conteúdo da proposta apresentada;
- Aprovar a política de segurança;
- Implementar a política de segurança;
- Manter, periodicamente, a política de segurança, procurando identificar as melhorias necessárias e efetuar as revisões cabíveis.

A seguir, cada uma das fases citadas será detalhada.

Identificar a legislação

Toda organização é submetida a várias leis, regulamentações, normas do órgão regulamentador da sua área de negócios, que devem ser seguidas e atendidas sob o risco grave de penalidades no caso de não cumprimento. Assim, é importantíssimo o levantamento de toda legislação para que as políticas de segurança não venham a atentar contra qualquer uma delas.

Exercício de fixação 3
Identificar a legislação

Qual a importância da identificação da legislação para o desenvolvimento da política de segurança?

Identificação dos recursos críticos

- Hardware.
- Software.
- Dados.
- Pessoas.
- Documentação.
- Suprimentos.
- Entre outros.

A primeira fase do processo de implantação de uma política de segurança compreende a identificação dos recursos críticos da organização, ou seja, aqueles recursos sob risco de segurança.

Por exemplo, considerando cenários da tecnologia da informação, podemos apresentar os seguintes recursos como críticos:

- Hardware, tais como servidores, equipamentos de interconexão (roteadores, comutadores etc.), linhas de comunicação, entre outros;
- Software, tais como Sistemas Operacionais, aplicativos, ferramentas de auxílio a atividades de negócio, utilitários etc.;
- Dados (em processamento ou em transmissão), backups, logs, bases de dados etc.;
- Pessoas, em termos de usuários (internos e externos, quando conveniente), funcionários e dirigentes;
- Documentação a respeito de softwares, sistemas de informação, entre outros;
- Suprimentos, tais como papel, fitas magnéticas, CDs/DVDs etc.

Considerando um cenário diferente, outros tipos de recursos podem ser levantados.

Exercício de fixação 4
Identificação dos recursos críticos

Cite dois recursos críticos da sua organização que devem ser levados em conta no processo de desenvolvimento da política de segurança.

_____

_____

_____

_____

Análise das necessidades de segurança

Engloba a análise de riscos:

- Ameaças e impactos.

Busca-se identificar:

- Componentes críticos.
- Grau de proteção adequado.
- Custos potenciais.
- Adequação às boas práticas.

Ao analisar as necessidades de segurança, deve-se considerar a análise de riscos, em especial as ameaças e impactos, de modo a determinar os elementos críticos na organização, os custos associados e o grau de segurança adequado.

A análise de riscos completa e correta é o ponto-chave para a política de segurança adequada a uma organização e, consequentemente, para a gestão da segurança da informação. A gestão de riscos será detalhada nos capítulos 6 e 7, incluindo mais informações a respeito da análise de riscos.

Outro ponto a ser observado são as recomendações das boas práticas existentes na área de segurança da informação. Seguir essas boas práticas colaborará para que a organização seja vista como preocupada com a segurança da sua informação.

Elaboração da proposta e discussão aberta

A proposta deve contemplar:

- Recursos críticos.
- Análise das necessidades de segurança.

A proposta deve ser discutida entre os envolvidos:

- Dirigentes da organização, em especial.

A proposta de política de segurança de uma organização deve ser elaborada com base no levantamento de recursos críticos e na análise das necessidades de segurança realizadas previamente para que, assim, os objetivos de segurança sejam identificados de maneira adequada, de acordo com o negócio e os riscos que envolvem a organização.

A política de segurança deve, normalmente, ser desenvolvida e apresentada pelo Comitê de Segurança da Informação. Esse comitê contará com representantes de várias áreas, principalmente a área jurídica, TI e RH, e deverá ter um período estabelecido.

Uma vez elaborada, a proposta deve ser discutida abertamente com todos os funcionários envolvidos diretamente com o assunto e, em especial, com os dirigentes da organização, uma vez que o apoio deles é crucial para a implantação da política de segurança.

Exercício de fixação 5
Elaboração da proposta

Quem desenvolverá a política de segurança da sua organização?

Documentação

- Definição de segurança da informação, suas metas, escopo e importância.
- Declaração do comprometimento dos dirigentes da organização.
- Objetivos de controle e os devidos controles.
- Análise, avaliação e gerenciamento de riscos.
- Explanação resumida das políticas, princípios, normas e requisitos.
- Definição das responsabilidades gerais e específicas quanto à gestão da segurança.
- Referências a documentos que apoiem a política.

A política de segurança de uma organização deve ser documentada, e o documento gerado deve ser aprovado por seus dirigentes para que possa ser publicado e divulgado para todos os envolvidos. Vale ressaltar a necessidade de a política de segurança estar alinhada aos objetivos e estratégias de negócio da organização.

O conteúdo da política de segurança deve conter, por recomendação da norma ABNT NBR ISO/IEC 27002:2013, os seguintes itens:

- Definição de segurança da informação, suas metas, escopo e relevância para a organização;
- Declaração do comprometimento dos dirigentes da organização com a política de segurança;
- Indicação dos objetivos de controle e dos controles, incluindo a análise/avaliação e gerenciamento dos riscos;
- Explicação sucinta a respeito das políticas, princípios, normas e requisitos necessários para garantir conformidade com a legislação, regulamentos, contratos e normas de segurança;
- Definição das responsabilidades para com a gestão da segurança da informação;
- Referências a documentos que apoiem a política de segurança.

Vale ressaltar que a política de segurança pode ser composta por várias políticas específicas, tais como política de senhas, de backup etc.

Aprovação e implementação

- Aprovação, em especial dos dirigentes da organização.
- Implementação.

A fase de aprovação da política de segurança corresponde ao resultado positivo conseguido após a análise da proposta elaborada e apresentada à organização. Em particular, exige-se o apoio por parte dos dirigentes da organização como uma forma de garantir os primeiros passos para a implementação da política de segurança e as condições adequadas à sua manutenção.

Na implementação, devem ser considerados todos os aspectos relacionados à implantação dos mecanismos de segurança (soluções técnicas, administrativas etc.) apropriados para assegurar que as necessidades de segurança levantadas previamente sejam atendidas a contento na organização.

Exercício de fixação 6
Aprovação e implementação

Quem aprovará a política de segurança da sua organização?

Comunicação da política e treinamento

A divulgação da política de segurança e sua comunicação a toda a organização é outro aspecto importante para sua implementação. Recomenda-se, a propósito, que a divulgação faça parte de programas de formação de funcionários novatos e de reciclagem dos antigos, além de ser efetuada periodicamente. Essa divulgação da política deve ser formal e efetiva, informando todos os detalhes da sua implementação, como deve ser cumprida e as penalidades, se for o caso, da sua não observância. Lembre-se de que a melhor medida de prevenção é a educação.

Manutenção

A política de segurança deve ser analisada periodicamente ou quando ocorrerem mudanças significativas. Deve considerar:

- Oportunidades para melhoria.
- Mudanças no ambiente organizacional (negócios, legislação ou tecnologias).
- Tendências de ameaças e vulnerabilidades.
- Incidentes de segurança ocorridos.

A política de segurança da informação adotada em uma organização deve ser periodicamente analisada (recomenda-se anualmente), com o objetivo de manter sua adequação e eficiência. Também deve ser revista nos casos de mudanças significativas em termos de negócios e avanços tecnológicos. Na análise, busca-se:

- Melhorias para a própria política, melhorias de controles, alocação de recursos e atribuição de responsabilidades;
- Atender a mudanças nos negócios, recursos disponíveis, condições técnicas e tecnológicas;
- Apresentar uma resposta a mudanças que afetam diretamente o modo de gerenciar a segurança da informação;
- Atender a mudanças em aspectos contratuais, regulamentares e legais;
- Atender a recomendações de autoridades ou órgãos relevantes.

Recomenda-se que tal análise seja efetuada por um funcionário ou equipe responsável pela gestão da política de segurança. Em seguida, deve-se gerar o novo documento da política de segurança e este, por sua vez, deve ser reconhecido e apoiado pelos dirigentes da organização.

Exercício de fixação 7
Manutenção

Como deve ser definido o tempo para manutenção de uma política de segurança?

Boas práticas

- Apoio explícito da alta direção.
- Determinar o que fazer para cada tipo de potencial violação à política de segurança.
- Estabelecer uma estrutura organizacional de responsabilidades.
- Estabelecer procedimentos de segurança de pessoal.
- Informar a todos os envolvidos os riscos e suas responsabilidades.

A política de segurança tem um papel determinante nas organizações e, por sua vez, é recomendável considerá-la como um conjunto de regras a ser fielmente seguido e gerido de maneira adequada. Sendo assim, torna-se evidente a relação entre a gestão da segurança da informação e a política de segurança de uma organização.

Com o objetivo de obter melhores resultados, são recomendadas as seguintes boas práticas, ao considerar a política de segurança de uma organização:

- A alta direção da organização deve apoiar e acreditar que as políticas de segurança da informação vão proteger as suas informações. Assim, o patrocínio da alta direção é importante para que os objetivos da política de segurança sejam alcançados. Esse apoio deve iniciar com o desenvolvimento da política, passar por sua assinatura e divulgação, chegando até a manutenção da eficiência e da sua atualização.
- Nem sempre é possível detectar uma violação à política de segurança; todavia, em situações nas quais haja possibilidade, é relevante identificar a causa em primeira instância, como erro, negligência, desconhecimento da política etc. Recomenda-se, ainda, que na própria política de segurança constem os procedimentos a serem seguidos caso uma violação aconteça, de acordo com sua gravidade, determinando, ainda, as ações corretivas necessárias e a punição dos responsáveis diretos pelo problema. Note que, assim como já citado no capítulo 2, a punição pode variar dependendo da infração, podendo ser levada à alçada da justiça; todavia, cabe à instituição divulgar a política de segurança, a legislação vigente e as responsabilidades específicas a todos os seus funcionários.
- É salutar estabelecer uma estrutura organizacional responsável pela segurança da informação na organização, com o intuito de definir os responsáveis por aprovar, revisar e gerenciar a implantação da política de segurança na organização. Tais atividades podem ser efetuadas por um funcionário ou equipe.
- Deve-se trabalhar a segurança de pessoal visando minimizar ou até mesmo evitar problemas de segurança da informação com causa proveniente de erros humanos.

Todos os integrantes da organização devem ter conhecimento a respeito dos riscos de segurança e das suas responsabilidades perante a questão da segurança. Com isso, é sempre recomendável a divulgação de boas práticas, normas, legislação e padrões vigentes.

Boas práticas

- Controlar e classificar os recursos computacionais disponíveis.
- Estabelecer controles de acesso lógico e físico.
- Administrar os recursos computacionais segundo os requisitos de segurança.
- Auditar a segurança periodicamente.

O controle e a classificação dos recursos computacionais da organização são relevantes. A classificação é efetuada de acordo com as condições críticas do recurso para os negócios. Em particular, deve-se associar cada recurso a um responsável direto na organização.

Recomenda-se a implantação de controles de acesso lógico e físico que estabeleçam os limites de acesso, estes controlados por dispositivos de controle de entrada e saída. Quanto aos recursos computacionais e demais ativos da organização, é importante administrá-los segundo os requisitos vigentes de segurança da informação.

A auditoria de segurança da informação deve ser uma atividade periódica na organização, a fim de verificar se a política de segurança está sendo eficiente e se há necessidade de atualizações.

Boas práticas para escrever o texto da política

- Definir o objetivo do documento.
- Usar textos curtos e objetivos, escritos na linguagem do público da organização.
- Definir papéis e responsabilidades.
- Evitar o uso de termos técnicos ou em língua estrangeira.
- Evitar o uso de “não”.
- Evitar o uso de “exceto” ou “em princípio”.
- Criar na política um item para as definições e conceitos.
- Penalização. Utilizar a colaboração do Jurídico e do RH.
- Criar regras e recomendações factíveis de serem aplicadas e cumpridas.
- Atentar para a correção gramatical. Evitar gírias e termos de duplo sentido.
- Solicitar que o Jurídico da organização avalie.

- Definir o objetivo do documento: descrever qual o objetivo do documento e o que a organização deseja comunicar com o documento da política;
- Usar textos curtos e objetivos, escritos na linguagem do público da organização. Seja claro na mensagem que deseja passar, de tal forma que o texto seja entendido por todos. Seja explícito e não deixe dúvidas ou incertezas;
- Definir papéis e responsabilidades com relação à política de segurança;
- Evitar o uso de termos técnicos ou em língua estrangeira. Ninguém é obrigado a conhecer a terminologia técnica que não é da sua área de atuação;
- Evitar o uso de “não”. Caso necessário utilizar “é proibido”, “negar”, “é vedado”, entre outras;
- Evitar o uso de “exceto” ou “em princípio”. Esses termos deixam a abertura para desculpas por não cumprimento;
- Criar na política um item para as definições e conceitos. Definir no início do documento todos os conceitos, definições, termos técnicos e siglas que serão empregados nas políticas;
- Penalização. Definir as possíveis penalidades para aqueles usuários que não cumprirem a política. Utilizar a colaboração do Jurídico e do RH;
- Criar regras e recomendações factíveis de serem aplicadas e cumpridas por toda a organização e em todos os níveis hierárquicos;
- Atentar para a correção gramatical. As políticas devem ser exemplo da apresentação escrita da linguagem. Evitar gírias e termos de duplo sentido;
- Solicitar que o Jurídico da organização avalie e aponha o seu “de acordo”.

Diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da APF

O DSIC publicou em 30 de junho de 2009 a norma complementar 03/IN01/DSIC/GSIPR, que apresenta as diretrizes para a elaboração das políticas de segurança da informação para a Administração Pública Federal (APF), do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR).

Na norma complementar 03/IN01/DSIC/GSIPR consta como deve ser a elaboração da política na APF, recomendando itens a serem contemplados (5.3 da norma complementar). É importante observar que ela institui:

- Gestor de Segurança da Informação e Comunicações do órgão ou entidade da APF;
- Comitê de Segurança da Informação e Comunicações do órgão ou entidade da APF;
- Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do órgão ou entidade da APF.

É fundamental a leitura do documento na íntegra, que deve ser acessado em: http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf

Roteiro de Atividades 4

Atividade 4.1 – Entendendo a política de segurança da informação

Segundo a norma NBR ISO/IEC 27002:2013, qual o objetivo de controle da política de segurança da informação?

Segundo a norma NBR ISO/IEC 27002:2013, quais as diretrizes para a implementação de uma política de segurança?

Atividade 4.2 – Elaborando uma política de segurança da informação

Você foi designado(a) para apresentar uma proposta de política de segurança para o serviço de correio eletrônico na sua instituição. Descreva e justifique as etapas que adotará para concluir uma proposta:

Quem deverá aprovar sua proposta? Justifique sua resposta.

Atividade 4.3 – Implementando uma política de segurança

Qual a atividade essencial após a conclusão e aprovação da política?
Apresente a sua justificativa.

Atividade 4.4 – Desenvolvendo uma política de segurança na sua organização

Como responsável pela área de TI, você foi designado(a) para compor o Comitê de Segurança da Informação da sua organização. O comitê atualmente está fazendo a revisão de alguns textos de políticas de segurança.

1. Analise os textos da política a seguir, aponte os erros existentes e reescreva-os:

a. Os usuários não devem empregar clientes de Internet Service Provider (ISP) e linhas dial-up para acessar a internet com os computadores da organização X. Toda atividade de acesso à internet deve passar através dos firewalls da organização X, de modo que os controles de acesso e os mecanismos de segurança possam ser aplicados.

b. Um documento que possua informação classificada como secreta ou altamente confidencial nunca pode ser enviada a uma impressora da rede sem que lá esteja uma pessoa autorizada para proteger sua confidencialidade durante e após a impressão.

c. Os geradores secundários e backup de energia devem ser empregados onde seja necessário para assegurar a continuidade dos serviços durante falhas ou falta de energia elétrica.

2. Em uma reunião do comitê, foi perguntado a você, como especialista no assunto, que apresentasse quais devem ser as primeiras políticas de segurança a serem trabalhadas e desenvolvidas. Qual a sua resposta? Justifique.

5

Gestão de riscos

objetivos

Entender, descrever e avaliar o processo de gestão de riscos.

conceitos

Definição de gestão de riscos, análise/avaliação de risco e aceitação, tratamento e comunicação de riscos.

Definições

- Risco.
- Gestão de riscos.
- Análise de riscos.
- Avaliação de riscos.
- Aceitação de riscos.
- Tratamento de riscos.
- Comunicação de riscos.

Exercício de nivelamento 1 
Gestão de riscos

O que é risco para você?

O que você entende por gestão de riscos?

Risco de segurança é uma combinação de ameaças, vulnerabilidades e impactos. Ameaças são eventos que exploram vulnerabilidades (fragilidades) e podem causar danos. O impacto é a consequência de uma vulnerabilidade ter sido explorada por uma ameaça.

No tocante à gestão de riscos, algumas definições são consideradas importantes e são apresentadas a seguir:

- A gestão de riscos compreende todas as ações tomadas para controlar os riscos em uma organização, incluindo análise/avaliação, tratamento, aceitação e comunicação dos riscos;

- A análise de riscos identifica e estima riscos, considerando o uso sistemático de informações. Engloba a análise de ameaças, vulnerabilidades e impactos, e é considerada o ponto-chave da política de segurança da informação de uma organização;
- A avaliação de riscos compara o risco estimado na análise com critérios predefinidos, objetivando identificar a importância do risco para a organização;
- A aceitação de riscos engloba o levantamento do nível aceitável de riscos para uma organização de acordo com seus requisitos específicos de negócio e segurança;
- O tratamento de riscos corresponde à seleção e implementação de medidas para modificar um dado risco.

A comunicação de riscos envolve as iniciativas de divulgação dos riscos aos funcionários, dirigentes e terceiros (estes últimos, quando cabível e necessário).

Questões determinantes

- Identificar ameaças.
- Identificar impactos.
- Determinar a probabilidade de concretização de ameaças.
- Entender os riscos potenciais.
- Classificar os riscos:
  - Por nível de importância.
  - Por grau de severidade das perdas.
  - Por custos envolvidos.

Para realizar uma efetiva gestão de riscos, é preciso levantar, inicialmente, as ameaças e impactos, a probabilidade de concretização de ameaças e os riscos potenciais. É recomendável classificar os riscos segundo os critérios: nível de importância, grau de severidade de perdas e custos envolvidos com a prevenção ou recuperação após desastres.

Se o custo para a prevenção de uma ameaça for maior que seu dano potencial, é aconselhável considerar outras medidas. As decisões devem ser tomadas considerando-se a importância do ativo ameaçado para a continuidade dos negócios da organização.

Observe que a análise de ameaças e vulnerabilidades procura identificar a probabilidade de ocorrência de cada evento adverso e as consequências do dano causado, enquanto a análise de impactos deve identificar os recursos críticos para a organização, isto é, aqueles que mais sofrerão com os danos.

Uma vez que é bastante difícil definir com precisão a probabilidade de uma ameaça ocorrer e os respectivos danos causados, recomenda-se estabelecer uma lista de ameaças potenciais, de recursos impactados, de requisitos de segurança afetados e grau de impacto (por exemplo, altíssimo, alto, moderado, baixo e muito baixo).

Gestão de riscos

Implementar em três níveis:

- 1º nível – Tecnologia.
- 2º nível – Processos.
- 3º nível – Pessoas.

Figura 5.1 Sequência para a mudança de conduta e prevenção dos riscos.

A gestão de riscos deve considerar os três níveis a seguir para sua implementação: tecnologias, processos e pessoas. A tecnologia garante a adequação técnica necessária ao tratamento adequado dos riscos; os processos asseguram que as atividades que compreendem a gestão de riscos sejam consideradas de forma sistemática; e, por fim, as pessoas, de modo que os funcionários e dirigentes identifiquem suas responsabilidades, conheçam os riscos e possam ajudar no sentido de sua redução e controle. Instrumentos como a política de segurança da informação e um código de conduta são recomendados no contexto.

Em termos das medidas de segurança, recomenda-se atenção para as seguintes categorias: preventivas, em caráter estrutural (por exemplo, uma política formal de controle de acesso lógico); corretivas, em caráter emergencial (planos de contingência, por exemplo); e orientativas, em caráter educacional (treinamentos, cartilhas, palestras etc.).

Em particular, lembre-se de que a orientação e a informação são essenciais para a redução de riscos. Portanto, atente para a importância do seguinte fluxo de gestão de riscos: informação – conhecimento – mudança de conduta – educação – prevenção dos riscos.

Exercício de fixação 1
Gestão de riscos

Quais os três níveis a considerar na gestão de riscos?

Análise e avaliação de riscos

- O que proteger?
- Quais as vulnerabilidades e ameaças?
- Como analisar?
  - Análise de impacto.
  - Probabilidades de ameaça.
  - Matriz de relacionamentos.
  - Cálculo dos riscos.
  - Avaliação de riscos.

Neste tópico, serão apresentados os aspectos relevantes para a análise/avaliação de riscos nas organizações. Em especial, serão apresentadas algumas classificações para as análises de impacto, definição de probabilidades e cálculos de riscos.

Identifica, quantifica/qualifica e prioriza os riscos de segurança da informação.
Essencial para:

- Gestão de riscos.
- Proposição de medidas de segurança adequadas.

Considerações:

- Devem ser sistemáticas.
- Devem usar métodos específicos.
- Devem ser realizadas periodicamente.

A análise/avaliação de riscos envolve a identificação, quantificação e qualificação dos riscos de segurança da informação, tendo como base os objetivos da organização. Envolve ainda a priorização de riscos, considerando os critérios de riscos aceitáveis. É uma atividade que indica como proceder para assegurar uma adequada gestão de riscos de segurança da informação e um apropriado conjunto de medidas de segurança para a organização em questão.

Algumas considerações quanto à análise/avaliação de riscos devem ser contempladas:

- Devem ser realizadas de modo sistemático, com o objetivo de identificar os riscos (análise) e qualificar os riscos (avaliação). A análise de riscos mede ameaças, vulnerabilidades e impactos em determinado ambiente, a fim de guiar a adoção de medidas apropriadas aos negócios e aos requisitos de segurança da organização;
- Devem usar métodos específicos que permitam a comparação entre resultados obtidos, bem como sua reprodução;
- Devem ser realizadas periodicamente, ou sempre que os requisitos de segurança, ativos, vulnerabilidades e/ou objetivos de negócio sofrerem alguma mudança.

Analisando os riscos

Considerar:

- Danos causados por falhas de segurança.
- Probabilidade de falhas ocorrerem.

Questões relevantes:

- O que proteger?
- Quais as vulnerabilidades e ameaças?
- Como analisar?

Resultado:

- Dados que guiam a gestão de riscos.

Na análise de riscos, deve-se considerar os danos prováveis aos negócios, resultantes de falhas de segurança; a probabilidade de falhas ocorrerem frente às vulnerabilidades e ameaças existentes; e as medidas de segurança implementadas (quando for o caso) de forma que, ao final, sejam levantados os dados necessários a uma adequada gestão de riscos.

Nesse sentido, algumas questões devem ser respondidas:

- O que proteger?
- Quais as vulnerabilidades e ameaças?
- Como analisar?

A resposta a essas questões é essencial para a execução e geração de resultados na análise de riscos.

O que proteger?

Deve-se analisar as ameaças e vulnerabilidades antes. Ativos típicos:

- Hardware.
- Software.
- Dados.
- Pessoas.
- Documentos.
- Sistemas de informação.
- Valores intangíveis.
- Contratos etc.

Nesta fase, devem ser considerados todos os ativos envolvidos no escopo do SGSI da organização, em especial aqueles diretamente relacionados aos objetivos de negócios. Portanto, trata-se de uma fase que não pode ser subjetiva, isto é, recomenda-se fazer um levantamento cuidadoso dos ativos, levando-se em conta parâmetros e categorias de seleção, por exemplo.

Em particular, deve-se analisar antes as ameaças e vulnerabilidades dos ativos que se quer proteger, de modo que sejam levantados todos os eventos adversos que possam, porventura, explorar as fragilidades de segurança da organização, causando danos.

São exemplos de ativos considerados cruciais aos negócios da organização: hardware, software, dados, pessoas, documentos, sistemas de informação, contratos, entre outros.

Exercício de fixação 2
O que proteger

Cite exemplos de ativos críticos na sua organização.

Vulnerabilidades e ameaças

- Determinar as vulnerabilidades e ameaças aos ativos a proteger.
- Determinar o impacto.
- Considerar:
  - Compromisso com a informação.
  - Confidencialidade.
  - Integridade.
  - Disponibilidade.

Após identificar os ativos que devem ser protegidos na organização, deve-se levantar as probabilidades de cada ativo estar vulnerável a ameaças. Para tanto, deve-se atentar para o compromisso com as informações, criando listas de prioridade, por exemplo; e para o comprometimento potencial de serviços de segurança, tais como confidencialidade, integridade e disponibilidade.

Exemplos de ameaças típicas:

- Desastres naturais.
- Falhas no fornecimento de energia elétrica.
- Roubo.
- Ameaças programadas.
- Falhas de hardware.
- Falhas de software.
- Erros humanos.

A seguir, são apresentadas algumas ameaças típicas em ambientes de TI:

- Desastres naturais que afetam a instalação física da organização. Durante o desastre, os controles de acesso físico podem ser comprometidos e alguns recursos com informações confidenciais podem ser violados com facilidade;
- Falhas no fornecimento de energia elétrica, que afetam parte do hardware da organização. Com o hardware danificado, os serviços tornam-se indisponíveis;
- Ameaças programadas, como vírus e bombas lógicas, que afetam softwares. Com isso, códigos não autorizados podem revelar ao mundo externo informações confidenciais, tais como senhas;
- Falhas de hardware. Com isso, o equipamento comprometido pode ser enviado para manutenção sem o cuidado prévio de apagar informações confidenciais nele contidas;
- Falhas de software, corrompendo dados;
- Erros humanos que afetam qualquer sistema da organização, permitindo, assim, a revelação de informações confidenciais; por exemplo, imprimir informações confidenciais em uma impressora pública.

Analisar considerando:

- Custos.
- Nível de proteção requerido.
- Facilidades de uso.

A análise de risco pode ser:

- Qualitativa.
- Quantitativa.

A análise de riscos deve medir as ameaças, vulnerabilidades e impactos de modo que o resultado possa servir como guia para a adoção de medidas de segurança adequadas aos requisitos de negócio da organização, considerando-se, para tanto, custos associados, nível de proteção requisitado pelos ativos e facilidades de uso.

Em particular, pode-se considerar a análise de risco sob termos qualitativos, objetivando atender aos requisitos de negócio, ou sob termos quantitativos, com o intuito de assegurar que os custos com medidas preventivas, corretivas e orientativas não ultrapassem o valor do ativo em questão, no que se refere ao patrimônio da organização e também à continuidade dos negócios.

Tipo de dado	Classificação	Importância
Resultado clínico	Pesquisa	Alto
Pesquisa de mercado	Pesquisa	Baixo
Patentes dependentes	Proprietária	Alto
Memorandos	Administrativo	Baixo
Salários de empregados	Financeira	Médio
Característica de novo produto	Proprietária	Médio

Tabela 5.1
Exemplo para dados de determinada organização.

No exemplo, considerou-se o ativo "Dados" e, ainda, os objetivos de negócio de determinada organização para estabelecer uma classificação dos dados (administrativa, financeira, cliente, pesquisa, proprietária) e a devida importância atribuída a cada categoria.

Análise de impactos

Pode considerar o impacto em curto e longo prazo. Exemplo de classificação:

- 0 – irrelevante.
- 1 – efeito pouco significativo.
- 2 – sistemas não disponíveis por determinado período.
- 3 – perdas financeiras.
- 4 – efeitos desastrosos, sem comprometimento dos negócios.
- 5 – efeitos desastrosos, comprometendo os negócios.

Impacto é a consequência de uma ameaça quando ela ocorre. Sendo assim, por exemplo, considerando controles de acesso inadequados, podemos citar impactos como a alteração não autorizada de dados e aplicativos, e a divulgação não autorizada de informações, que, por sua vez, causam problemas diretos à organização. Sendo assim, é importante analisar os impactos, visando uma adequada gestão de riscos na organização.

Para analisar impactos, pode-se considerar uma proposta de classificação específica de apoio. Tipicamente, os impactos causados por ameaças à organização são analisados sob dois aspectos: curto e longo prazo, considerando o tempo em que um dado impacto permanece afetando os negócios.

Neste contexto, pode-se considerar a seguinte proposta para categorizar impactos:

- 0, impacto irrelevante;
- 1, efeito pouco significativo que não afeta a maioria dos processos de negócios da instituição;
- 2, sistemas não disponíveis por determinado período de tempo, podendo causar perdas de credibilidade e imagem comercial, além de pequenas perdas financeiras;
- 3, perdas financeiras de maior vulto e perda de clientes;
- 4, efeitos desastrosos, mas que não comprometem a sobrevivência da organização;
- 5, efeitos desastrosos que comprometem a sobrevivência da organização.

Exercício de fixação 3
Análise de impacto

Explique o que é uma análise de impacto.

Matriz de relacionamentos

Ameaças	Impacto	Probabilidade
Erros humanos		
Instalação de hardware e software não autorizados		
Códigos maliciosos		
Bugs dos Sistemas Operacionais		
Invasão		
Desastres naturais		
Desastres causados por pessoas		
Falhas em equipamentos		
Sabotagem		
Grampo telefônico		
Monitoramento de tráfego na rede		
Modificação de informações		
Acesso a arquivos de senhas		
Uso de senhas frágeis		
Usuários internos praticando atos ilegais		

Tabela 5.2
Ameaças x Impactos x Probabilidades.

A matriz de relacionamentos é um modo simplificado de visualização das ameaças, impactos e probabilidades de acordo com o exemplo proposto, isto é, relacionando, para cada ameaça potencial na organização, seu impacto e probabilidade de ocorrência. Por exemplo, podem ser utilizadas as categorias de 0 a 5 para cada item, conforme apresentado anteriormente.

Exercício de fixação 4
Matriz de relacionamento

Preencha a tabela anterior de Ameaças x Impacto x Probabilidade com valores de 0 a 5, de acordo com o ambiente de TI da sua organização.

Cálculo dos riscos

- Riscos são calculados a partir da relação entre impacto e probabilidade de ocorrência.
- Considerando as propostas de classificação anteriores:
  - 0 (valor mínimo), nenhum risco.
  - 25 (valor máximo), risco altíssimo.
- Quanto maior o risco, maior a importância de se aplicar uma medida de segurança específica.

Riscos são calculados a partir da relação entre impacto e probabilidade de ocorrência, ou seja, risco = impacto * probabilidade.

Em particular, considerando as classificações propostas para impacto e probabilidade anteriormente apresentadas, ao efetuar a multiplicação, obtém-se uma faixa de valores para o risco de 0 (nenhum risco) até 25 (risco altíssimo). Pode-se, então, considerar essa proposta geral, por exemplo, para calcular os riscos gerais da organização e propor medidas de segurança adequadas a seu devido tratamento, considerando, para tanto, um nível aceitável de riscos, já que nem todos os riscos, devido aos custos, têm a garantia de serem reduzidos por meio de medidas de segurança.

Avaliação de riscos

Modos:

- Qualitativo.
- Quantitativo.

Conhecer os impactos é relevante.

Ao avaliar riscos, procura-se uma base que sirva para efeitos de comparação; por exemplo, análise e avaliação de riscos efetuadas em épocas anteriores. O conhecimento prévio de impactos e probabilidades de riscos é sempre relevante para uma avaliação adequada e completa.

Por outro lado, há basicamente dois modos de realizar a avaliação de riscos:

- **Qualitativo**: a avaliação de riscos através da estimativa qualitativa é aquela que utiliza atributos qualificadores e descritivos para avaliar. Não são atribuídos valores financeiros. É considerada muito subjetiva. Exemplo: Alto, Média, Baixa e Muito Baixa;
- **Quantitativo**: a avaliação de riscos através da estimativa quantitativa é aquela que utiliza valores numéricos financeiros para cada um dos componentes coletados durante a identificação dos riscos. Exemplo: probabilidade de 50%; impacto: R$ 100.000,00.

Nos exemplos a seguir são mostradas duas análises de riscos realizadas no mesmo ambiente, mas com formas diferentes de cálculo do risco. Observe os critérios utilizados em cada uma.

Exemplo 1 – Análise de risco

Numa determinada instituição de ensino foi determinado que a área de TI realizasse um levantamento de riscos da rede administrativa em três departamentos: Engenharia, Financeiro e Administrativo. Para tanto, foi utilizado como metodologia o conceito de riscos como resultado da probabilidade vezes o impacto, tendo como parâmetros qualitativos alto, médio e baixo, com pesos atribuídos a cada um para o cálculo do risco. Após realizar a etapa de análise de riscos, você realizou a avaliação dos riscos, chegando ao resultado a seguir:

Área	Probabilidade de ocorrer		Impacto caso ocorra		Risco = P x I	
	Avaliação	Peso	Avaliação	Peso	Peso	Avaliação
Departamento de Engenharia	Média	2	Médio	2	4	Médio
Departamento Administrativo	Média	2	Baixo	1	2	Baixo
Departamento Financeiro	Média	2	Alto	3	6	Alto

Tabela 5.3
Resultado da avaliação de riscos.

Critério de Probabilidade		Peso
Alta	Tem ocorrido com frequência mensal	3
Média	Ocorreu pelo menos uma vez nos últimos seis meses	2
Baixa	Não existe registro/ histórico de ocorrência	1

Tabela 5.4
Critério de probabilidade utilizado.

Critério Impacto		Peso
Alto	Caso ocorra, causará grandes prejuízos financeiros	3
Médio	Na ocorrência seus prejuízos, causarão impacto financeiro de até R$ 10 mil	2
Baixo	Na ocorrência seus prejuízos, não causarão impacto financeiro	1

Tabela 5.5
Critério de impacto utilizado.

Risco	
Alto	>4
Médio	>2 e <=4
Baixo	<=2

Tabela 5.6
Critério de risco utilizado.

Exemplo 2 – Análise de risco

Numa determinada instituição da área de ensino, foi determinado que a área de TI realizasse um levantamento de riscos da rede administrativa em três departamentos: Engenharia, Financeiro e Administrativo. Para tanto, foi utilizada uma metodologia desenvolvida por uma consultoria que calcula os riscos da instituição através de uma fórmula que se utiliza de parâmetros como criticidade, disponibilidade, confidencialidade entre outros. Após realizar a etapa de análise de riscos, você realizou a avaliação dos riscos, chegando ao resultado a seguir:

Tabela 5.7
Resultado da avaliação de riscos.

Área	Criticidade da rede	Disponibilidade da rede	Confidencialidade da rede	Importância da rede	EO	ED	RR
Departamento de Engenharia	2	3	1	6	0,1	0,3	3,8
Departamento Administrativo	2	3	2	12	0,5	0,5	3
Departamento Financeiro	2	3	3	18	0,3	0,3	8,8

Valores para Criticidade, Disponibilidade e Confidencialidade	
Qual a criticidade desta rede para o negócio da área? Qual a importância do requisito Disponibilidade ou Confidencialidade para a segurança da rede na área?	
Alta	3
Média	2
Baixa	1

Tabela 5.8 Valores dos critérios para Criticidade, Disponibilidade e Confidencialidade.

Valores de EO e ED	
Muito baixo	0,1
Baixo	0,3
Moderado	0,5
Alto	0,7
Muito Alto	0,9

Tabela 5.9 Valores para evitar a ocorrência e a degradação.

Convenções		
IR	Importância da rede.	Qual a importância da rede para os negócios?
EO	Evitar a ocorrência.	Qual a probabilidade atual de evitar a ocorrência.
ED	Evitar a degradação.	Qual a possibilidade atual de evitar a degradação.
RR	Risco relativo	IR*[(1-EO)*(1-ED)] Cálculo do risco nesta metodologia.

Tabela 5.10 Convenções utilizadas.

Para o exemplo apresentado, o ativo analisado é a rede da organização. Como pode ser visto, algumas convenções foram utilizadas para mapear a importância de serviços específicos de segurança, tais como disponibilidade, integridade e confidencialidade em uma análise, e na outra apenas a probabilidade e o impacto. Ao final, o resultado expresso foi gerado a partir da proposta para a medição de riscos naquela organização.

Determina os critérios para indicar se um risco é aceitável. Aspectos a considerar:

- Requisitos legais e de segurança.
- Objetivos organizacionais.
- Custo x benefício.

Essa é uma atividade que objetiva determinar os critérios a considerar para indicar se um risco é aceitável ou não para a organização.

Um risco é considerado aceitável quando, por exemplo, após a avaliação, é considerado baixo ou seu tratamento representa custos inviáveis para a organização.

Para determinar se um risco é aceitável ou não, alguns aspectos devem ser levados em conta:

- Requisitos legais, regulamentares, contratuais e de segurança;
- Objetivos de negócio;
- Relação custo x benefício para a aquisição/implementação de medidas de segurança em relação aos riscos que devem ser reduzidos.

Exercício de fixação 5
Avaliação de riscos

O que é e como deve ser determinado o risco aceitável?

Tratamento de riscos de segurança

- Compreende a colaboração entre partes:
  - Dirigentes, funcionários, auditores, consultores etc.
- Objetivos:
  - Aprovar metodologias e procedimentos de segurança da informação.
  - Assegurar a conformidade com a política de segurança.
  - Coordenar a implantação de controles.
  - Educar para a segurança da informação.

Após a análise, avaliação e definição dos critérios aceitáveis para os riscos na organização, deve-se indicar o procedimento para tratar os riscos. Entre as alternativas de tratamento, destacam-se:

- Selecionar e implementar medidas de segurança adequadas para reduzir os riscos a um nível aceitável (de acordo com os critérios definidos na "Aceitação de riscos");
- Implementar medidas preventivas contra riscos, não permitindo que as vulnerabilidades sejam exploradas para a concretização do risco;
- Transferir os riscos para terceiros através de contratos com seguradoras, por exemplo.

Vale lembrar que os riscos de segurança variam de acordo com o local (cenário ou contexto) e, com isso, é importante considerar tal fato ao determinar as medidas de segurança mais adequadas.

Atenção para a aplicação de medidas de segurança, pois, dependendo da organização, estas podem ser inviáveis. Por exemplo, aplicar registros (logs) para todas as atividades dos usuários pode ir de encontro à legislação vigente e à privacidade das pessoas em seu ambiente de trabalho.

Vale ressaltar ainda que monitorar, avaliar e propor melhorias regularmente nas medidas de segurança e, por consequência, no tratamento de riscos, é uma prática recomendada para aumentar a eficácia da gestão de riscos na organização.

Exercício de fixação 6
Tratamento de riscos de segurança

Quais os objetivos do tratamento de riscos?

Aspectos importantes no tratamento de riscos:

- Metodologias e procedimentos de segurança da informação.
- Conformidade com a política de segurança.
- Medidas de segurança:
  - Corretivas.
  - Preventivas.
  - Orientativas.

O tratamento de riscos é uma atividade a ser realizada após a análise/avaliação de riscos da organização, com o objetivo de auxiliar na redução dos riscos até um nível aceitável. Sendo assim, o uso de procedimentos e medidas de segurança deve ser implementado nessa atividade, sejam medidas preventivas, corretivas ou orientativas.

Vale salientar que quaisquer medidas que envolvam monitoramento regular de pessoas e/ou sistemas devem ser implementadas conforme a legislação vigente.

Deve-se ainda atentar durante a fase do tratamento do risco para segmentos importantes para que sejam implementados controles e que devem constar do escopo do tratamento:

- Recursos humanos.
- Controles de acesso lógico.
- Controles de acesso físico.
- Controles ambientais.
- Comunicações.
- Continuidade de serviços.
- Contratação de serviços de terceiros.
- Controle organizacional.
- Controle de mudanças.

Em termos de tratamento de riscos de segurança, algumas áreas são consideradas essenciais à organização na garantia de seus objetivos de negócio. Destacam-se, entre tais áreas, preocupações com riscos, impactos e devido tratamento para Recursos Humanos, segurança de acesso e de comunicações, além dos negócios.

- Segurança de Recursos Humanos.
- Segurança de acesso.
- Segurança nas comunicações.
- Segurança e negócios.

Exercício de fixação 7
Tratamento de riscos

Quais as áreas essenciais da sua organização na garantia dos seus objetivos de negócio?

Neste tópico, serão apresentados vários exemplos de riscos, impactos e tratamentos adequados para assegurar que as organizações contemplem a segurança em termos de recursos humanos, controles de acesso, comunicações e negócios.

Vale ressaltar que há outras preocupações relevantes em relação a riscos e impactos de segurança nas organizações; outras informações sobre análise de riscos podem ser obtidas na norma ABNT NBR ISO/IEC 27005:2011 e aplicadas, independentemente do ramo de negócio das organizações. Essa norma é estudada em detalhes no curso Gestão de Riscos em TI.

Tratamento de riscos na segurança de Recursos Humanos

As pessoas devem ter consciência de suas responsabilidades e dos riscos e ameaças de segurança. Deve-se ainda atentar para eventos adversos que representem riscos.

Uma prática boa e recomendada para minimizar os riscos de segurança nas organizações é educar, conscientizar e treinar (quando for necessário) os recursos humanos: funcionários, terceiros, parceiros etc. Em particular, algumas práticas também auxiliam a atingir tal objetivo:

- Assegurar que as pessoas conheçam, entendam e respeitem suas responsabilidades para com a redução de riscos de segurança da organização, especialmente, em termos de roubos, fraudes e mau uso de recursos e informações;
- As pessoas devem estar conscientes de que é importante notificar seus superiores a respeito de quaisquer eventos adversos que representem riscos (potenciais ou reais) à segurança da organização;
- As pessoas devem conhecer as possíveis ameaças e riscos de segurança, de forma que entendam seu papel quanto à segurança da informação na organização. De modo especial, todos devem efetuar suas ações em conformidade com a política de segurança vigente, reduzindo, assim, a ocorrência de erros humanos e, consequentemente, os riscos.

Exercício de fixação 8

Tratamento de riscos na segurança de recursos humanos

Quais medidas você irá propor para o tratamento de riscos de segurança de recursos humanos na sua organização?

Tratamento de riscos na segurança de acesso

- Atentar para os fatores de risco.
- Considerar a análise/avaliação de riscos:
  - Definir perímetros de segurança.
  - Proteger equipamentos e dispositivos de armazenamento.
  - Minimizar riscos de corrupção de sistemas operacionais.
  - Reduzir riscos de ameaças físicas.
- Educação e conscientização são cruciais.

Ao considerar a segurança de acesso, inicialmente é relevante a preocupação com fatores de risco para o contexto, tais como as responsabilidades atribuídas a funcionários e terceiros, o valor dos ativos acessíveis e os direitos sobre o encerramento de atividades, por exemplo.

Nas organizações, o nível de proteção requerido pelos diversos controles de acesso é determinado em função da análise/avaliação de riscos. Sendo assim, deve-se atentar para os resultados obtidos com tal atividade para determinar medidas adequadas de segurança com o objetivo, por exemplo, de:

- Definir os perímetros de segurança para a segurança física e do ambiente;
- Proteger adequadamente os equipamentos (internos ou externos às dependências da organização) contra acessos não autorizados, perdas ou danos, perigos do próprio ambiente, vazamento de informações, entre outros;
- Avaliar se é adequado destruir determinado dispositivo que armazena informações críticas ao negócio da organização, ou se é cabível enviá-lo para conserto em local autorizado pelo fabricante do dispositivo;
- Minimizar os riscos de corrupção de Sistemas Operacionais, como garantir que sua atualização seja efetuada apenas por pessoas competentes e autorizadas para tal;
- Reduzir os riscos de ameaças como furtos, incêndios, explosões, poeira, efeitos químicos, enchentes, falhas no fornecimento de energia elétrica etc.
- A educação e a conscientização dos usuários é crucial para a segurança da informação, uma vez que a adequada utilização de recursos e informações, como "ferramentas" de trabalho, fortalece a cultura de segurança da organização como um todo.

Exemplos de riscos relacionados ao controle de acesso lógico inadequado:

- Alteração não autorizada de dados e aplicativos.
- Divulgação não autorizada de informações.
- Introdução de códigos maliciosos.

Impactos:

- Perdas financeiras decorrentes de fraudes, restaurações etc.
- Inviabilidade de continuidade dos negócios.

Há uma série de riscos diretamente relacionados ao controle inadequado de acesso lógico aos recursos e informações. Eis alguns exemplos: divulgação não autorizada de informações; modificações não autorizadas em dados e aplicativos e introdução de códigos maliciosos nos sistemas.

Sendo assim, a inexistência ou inadequação de controles de acesso lógico afeta diretamente os recursos e informações, aumentando os riscos. Além disso, os impactos podem ser maiores à medida que se consideram os aplicativos e informações críticas aos negócios da organização. Caso existam obrigações legais envolvidas com o controle de acesso lógico, a organização poderá sofrer ações judiciais.

Exemplos de tratamentos para um adequado controle de acesso lógico:

- Restringir e monitorar o acesso a recursos críticos.
- Utilizar criptografia.
- Não armazenar senhas em logs.
- Conscientizar os usuários para que não divulguem suas senhas.
- Conceder acesso apenas aos recursos necessários às atividades dos funcionários.

Conforme visto no exemplo anterior, é importante considerar medidas de segurança adequadas para efetuar o controle de acesso lógico nas organizações. Nesse sentido, algumas práticas são recomendadas:

- Restrição e monitoramento de acesso a recursos críticos da organização, tais como servidores, documentos etc;
- Utilizar criptografia forte, assegurando a confidencialidade das informações;
- Não armazenar senhas em logs, permitindo o acesso posterior por pessoas não autorizadas;
- Conscientizar as pessoas para que não divulguem suas senhas, verbalmente ou por e-mail, nem as armazenem em arquivos;
- Conceder acesso às pessoas apenas aos recursos realmente necessários para a execução de suas atividades.

Exemplos de riscos relacionados ao controle de acesso físico inadequado:

- Roubo de equipamentos.
- Atos de vandalismo.

Impactos:

- Perdas financeiras.
- Facilidades para ataques contra controles de acesso lógico.

Há vários riscos diretamente relacionados ao controle inadequado de acesso físico nas organizações. Alguns exemplos: roubo de equipamentos ou de seus componentes internos e atos de vandalismo, como cortes de cabos elétricos. Sendo assim, a inexistência ou inadequação de controles de acesso físico também pode facilitar a atuação de invasores que atacam diretamente os controles de acesso lógico aplicados aos recursos e informações.

Exemplos de tratamentos para um adequado controle de acesso físico:

- Identificar funcionários e visitantes.
- Controlar a entrada/saída de equipamentos.
- Supervisionar a atuação da equipe de limpeza, manutenção e vigilância.

Conforme visto no exemplo anterior, é importante considerar medidas de segurança adequadas para efetuar o controle de acesso físico nas organizações. Nesse sentido, algumas práticas são recomendadas:

- Estabelecer formas de identificação capazes de distinguir funcionários de visitantes;
- Controlar a entrada e a saída de equipamentos, registrando, por exemplo, data, horário e responsável;
- Supervisionar as atividades das equipes de limpeza, manutenção e vigilância, principalmente se terceirizadas.

Exemplos de riscos relacionados ao controle ambiental inadequado:

- Desastres naturais.
- Falhas no fornecimento de energia elétrica.

Impactos:

- Danos em equipamentos.
- Indisponibilidade de serviços.
- Perdas financeiras.

Há vários riscos diretamente relacionados ao controle ambiental inadequado ou inexistente. Como exemplos, considere desastres naturais e falhas no fornecimento de energia elétrica.

Os impactos compreendem danos em equipamentos, perdas de dados ou indisponibilidade de serviços, por exemplo, gerando perdas financeiras e de imagem comercial.

Exemplos de tratamentos para um adequado controle ambiental:

- Uso de material resistente a fogo.
- Manutenção de número suficiente de extintores de incêndio.
- Controle de focos de problemas com água.
- Controle de temperatura, umidade e ventilação.
- Manutenção da limpeza e conservação do ambiente.

Exercício de fixação 9
Tratamento de riscos na segurança de acesso

Que riscos na segurança de acesso você identifica dentro do seu ambiente na sua organização?

Quais medidas você vai propor para o tratamento de riscos na segurança de acesso na sua organização?

Tratamento de riscos na segurança das comunicações

- Disponibilizar medidas de segurança adequadas às comunicações.
- Considerações:
  - Proteção de conexões a serviços de rede.
  - Garantir a segurança para a comunicação wireless.

Para garantir a segurança nas comunicações, é relevante considerar a análise/avaliação de riscos, com o intuito de adequar as medidas de segurança aos requisitos de comunicação necessários aos negócios da organização. A gerência das comunicações também é recomendável.

Nesse contexto, algumas práticas são recomendadas:

- Proteger conexões que disponibilizem serviços de rede, principalmente aquelas que operam diretamente com informações e aplicações críticas para o negócio da organização;
- Identificar as medidas de segurança adequadas para a comunicação wireless, tais como autenticação forte e seleção de frequências;
- Definir a periodicidade da revisão dos direitos de acesso à rede e seus serviços, atribuídos a funcionários, colaboradores, terceiros etc.

Exercício de fixação 10

Tratamento de riscos na segurança das comunicações

Quais medidas você vai propor para o tratamento de riscos na segurança das comunicações da sua organização?

Tratamento de riscos e negócios

Proteger recursos e informações para atingir objetivos de negócio. Atentar para:

- Aplicações críticas aos negócios.
- Controlar novos contratos e parcerias.
- Identificar necessidades de integridade das mensagens.
- Estabelecer uma política para uso adequado de criptografia.
- Identificar e reduzir riscos à continuidade de negócios.

A segurança da informação deve ser adequada à garantia da proteção aos recursos e informações da organização, segundo seus objetivos de negócio. Nesse contexto, algumas considerações devem ser levadas em conta. Por exemplo:

- Atentar para riscos relacionados diretamente às aplicações críticas aos negócios, em termos, principalmente, do uso de recursos e informações compartilhadas;
- Controlar adequadamente novas situações que influenciem o compartilhamento de informações e recursos, tais como novos contratos ou parcerias, objetivando o tratamento de potenciais riscos de acesso não autorizado;
- Em termos do uso de criptografia, deve-se considerar o tipo e a qualidade de algoritmos adequados às necessidades. É aconselhável elaborar uma política específica que elucide o modo correto de uso, reduzindo os riscos de uso inadequado, por exemplo;
- Todas as mudanças devem ser controladas, e os riscos e impactos envolvidos devem ser considerados para determinar as medidas de segurança adequadas;
- Em particular, a gestão da continuidade de negócios deve incluir mecanismos para identificar e reduzir riscos, de forma a complementar a análise/avaliação global de riscos, auxiliando prontamente processos que necessitem de respostas imediatas.

Exemplo de risco relativo à continuidade de serviços:

- Backup irregular.

Impactos:

- Perdas financeiras.

Tratamento para a continuidade adequada de serviços:

- Política de backup.
- Conscientização dos funcionários.

As cópias de segurança (backups) são uma importante ferramenta de apoio à continuidade dos serviços e, por consequência, dos negócios; todavia, riscos associados a procedimentos inadequados de backup regular causam impactos como desperdício de tempo e recursos, e, por conseguinte, perdas financeiras. Sendo assim, medidas como uma política formal de backup e a promoção contínua de treinamento e conscientização dos funcionários

quanto à segurança (incluindo orientações sobre cópias de segurança pessoais) são recomendadas para as organizações.

Exemplo de risco relativo à contratação de serviços de terceiros:

- Não ter certeza de que o terceiro emprega medidas de segurança compatíveis.

Impactos:

- Perdas financeiras.
- Comprometimento dos negócios.

A seguir são apresentados alguns riscos e impactos diretamente relacionados a problemas com a contratação de serviços de terceiros. Entre os riscos, pode-se destacar a incerteza de que o terceiro (ou prestador de serviço) emprega medidas de segurança compatíveis com aquelas adotadas na organização, considerando como base todas as normas da organização.

Exemplos de tratamento para um adequado controle da contratação de terceiros:

- Definir cláusulas contratuais que responsabilizem o terceiro por questões de segurança.
- Definir cláusulas contratuais que possibilitem atualizações nos serviços e sistemas.

Para tratar riscos como os apresentados no exemplo anterior, algumas medidas são recomendadas: instituir cláusulas contratuais que definam claramente as responsabilidades do terceiro, visando a segurança da organização, além de incluir cláusulas contratuais que possibilitem alterações nos serviços e sistemas em função de novos objetivos de negócio.

Para pensar

Um contrato de prestação de serviços deve contemplar, pelo menos, os seguintes itens: custos básicos; direitos das partes (ao final do contrato); indenizações no caso de perdas; direitos de propriedade sobre as informações; direitos de propriedade intelectual; repasse de informações técnicas e documentações; possibilidade de alterações; padrões de segurança da organização e padrões de qualidade.

Exemplos de cláusula contratual de segurança da informação:
"Constitui obrigação da CONTRATADA sempre que utilizar sistema com interface com os sistemas da CONTRATANTE: quando solicitado por escrito pela CONTRATANTE, realizar prioritariamente as alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos sistemas que tenham sido comunicados pela CONTRATANTE."

Exemplos de riscos relativos ao controle organizacional inadequado:

- Violações de acesso não autorizadas.
- Planejamentos inadequados.

Impactos:

- Perda de informações.
- Desperdício de investimentos.

O controle organizacional compreende todos os aspectos relativos à proteção da organização, de acordo com seus objetivos de negócio e tendo como base os riscos, como: violação não autorizada de acesso a recursos e informações, roubo de equipamentos e planejamento inadequado do crescimento computacional.

Exemplos de tratamento para um adequado controle organizacional:

- Definir responsabilidades para cada cargo da hierarquia organizacional.
- Atender à legislação vigente.

Para o exemplo anterior, algumas recomendações quanto a medidas de segurança são diretamente aplicáveis:

- Definir as responsabilidades dos cargos em função da hierarquia organizacional, de modo que as atividades sejam devidamente realizadas.
- Atender à legislação vigente e aos requisitos contratuais e regulamentares relativos à segurança na organização.

Exemplos de riscos relativos ao controle inadequado de mudanças:

- Uso de hardware e software não autorizados.
- Dificuldades de manutenção.
- Mudanças inesperadas e acidentais.

Impactos:

- Incompatibilidades.
- Decisões equivocadas.
- Perdas financeiras.

Um controle de mudanças adequado para as organizações deve contemplar soluções para riscos, tais como:

- Uso de hardware e software não autorizados;
- Dificuldade de manutenção por falta de documentação e procedimentos específicos;
- Mudanças inesperadas ou acidentais.

Exemplos de tratamento para um adequado controle de mudanças:

- Documentar as alterações efetuadas.
- Avaliar o impacto de mudanças.
- Definir procedimentos de emergência.
- Planejar mudanças.

Algumas medidas de segurança para um adequado controle de mudanças são propostas a seguir:

- Documentar todas as alterações e atualizações efetuadas e implementá-las apenas com a devida autorização;
- Avaliar o impacto das mudanças antes de implementá-las;
- Definir o procedimento em situações de emergência;
- Planejar mudanças de modo a minimizar o impacto para o dia a dia da organização.

Comunicação de riscos

- Ativos são elementos essenciais ao negócio da organização.
- Ativos devem ser inventariados.
- Todo ativo deve ter um responsável por manter sua segurança.

Esta atividade engloba todas as ações para a divulgação dos riscos, de forma a informar e orientar os envolvidos, objetivando, assim, a redução (e muitas vezes, a eliminação) dos riscos na organização.

Roteiro de Atividades 5

Atividade 5.1 – Entendendo os conceitos de gestão de risco

Apresente os conceitos de gestão de risco a seguir e cite exemplos de cada fase:

Fase	Conceito	Exemplo
Análise de riscos		
Avaliação de riscos		
Aceitação de riscos		
Tratamento de riscos		
Comunicação de riscos		

Atividade 5.2 – Realizando a gestão de riscos

1. Explique o que é uma análise de impacto.

2. Como é calculado o risco? Justifique.

3. Quais são os modos de avaliação de riscos existentes?

4. Descreva o que significa “tratar o risco”.

Atividade 5.3 – Realizando a gestão de riscos

1. Descreva as atividades que você desenvolverá na sua organização para realizar a análise de risco. Quais serão os objetivos desta análise?

2. Considerando as atividades desenvolvidas anteriormente, analise um servidor de aplicação (ou o processo de controle de acesso físico) da sua organização apontando o que se pede:

a. 3 (três) ameaças.

b. 6 (seis) vulnerabilidades.

c. Probabilidade de cada vulnerabilidade ser explorada (Alta, Média ou Baixa).

d. Criticidade do ativo para os negócios da organização (Alta, Média ou Baixa).

e. Impacto para cada vulnerabilidade se explorada e concretizando a ameaça (Alta, Média ou Baixa).

f. Risco do ativo considerado (utilize os pesos, parâmetros e cálculo do exemplo anterior).

Atividade 5.4 – Realizando a gestão de riscos na sua organização

1. Apresente as necessidades de gestão de risco para sua organização. Justifique sua resposta.

2. Escreva um escopo inicial e relacione dois profissionais para compor a equipe de análise. Justifique sua resposta.

6

Gerência de operações e comunicações

objetivos

Descrever responsabilidades, selecionar e aplicar controles e procedimentos da gerência de operações e comunicações.

conceitos

Definição, procedimentos e responsabilidades da gerência de operações e comunicações e gerência de segurança de redes.

Exercício de nivelamento 1
Gerência de operações e comunicações

Qual o seu entendimento de gerência de operações e comunicações?

Como sua organização realiza a gerência de operações e comunicações?

Objetivos

- Assegurar que as operações sejam realizadas de acordo com os requisitos de segurança.
- Gerenciar os serviços terceirizados.
- Proteger contra códigos maliciosos.
- Prover cópias de segurança.
- Gerenciar a segurança das redes.
- Controlar o manuseio de mídias.
- Controlar a transferência de informações e softwares.
- Garantir o monitoramento global de operações e comunicações.

A gerência de operações e comunicações destina-se a assegurar que os requisitos de segurança da informação sejam atendidos, considerando-se a operação dos recursos computacionais e comunicações na organização.

Sendo assim, tal gerenciamento engloba o tratamento de serviços terceirizados, a proteção contra código malicioso, a política de cópias empregada, a segurança das redes, mídias

e transferência de softwares e informações, além do monitoramento global de todos os aspectos relacionados a operações e comunicações na organização.

Procedimentos e responsabilidades operacionais

- Documentar procedimentos operacionais.
- Controlar mudanças operacionais.
- Estabelecer procedimentos para o gerenciamento de incidentes.
- Segregar responsabilidades.
- Separar facilidades de desenvolvimento, testes e operação.

No tocante aos procedimentos e responsabilidades operacionais, algumas práticas são consideradas essenciais, com o objetivo de assegurar a adequação das operações aos requisitos de segurança da informação da organização. Tais práticas são detalhadas a seguir:

- Documentar procedimentos operacionais de modo formal e flexível (no sentido de permitir modificações, quando necessárias e autorizadas), englobando o tratamento de operações de manutenção, manipulação de erros e demais condições adversas, contratos de suporte, procedimentos de recuperação, geração de cópias de segurança, entre outros
- Controlar mudanças operacionais, definindo responsabilidades gerenciais e, sempre que praticável, integrar os procedimentos de controle de mudanças de aplicações e sistemas operacionais. É relevante manter registros de auditoria, quando mudanças forem efetuadas
- Estabelecer procedimentos para o gerenciamento de incidentes, como ação para assegurar uma resposta rápida, efetiva e ordenada aos incidentes de segurança
- Segregar responsabilidades, com o objetivo de reduzir riscos de má utilização dos sistemas, por exemplo, impedindo que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização. Sendo assim, é importante separar o gerenciamento de certas responsabilidades ou áreas de responsabilidade, de forma que as possibilidades de modificações não autorizadas sejam reduzidas
- Separar facilidades de desenvolvimento, testes e operação, indicando um nível de separação necessário para prevenir problemas operacionais, principalmente em termos de acessos ou modificações não autorizadas. Por exemplo, as regras para a mudança do estado de um software (desenvolvimento para produção) devem ser definidas e documentadas.

Exemplo: Tratando responsabilidades operacionais:

- "Os usuários que operam os sistemas de TI da organização devem assinar um termo de responsabilidade antes de obter acesso a eles. A assinatura do termo representa que o usuário entende e concorda com as políticas e normas de segurança e tem conhecimento a respeito da legislação vigente e aplicável aos casos de não cumprimento."
- No exemplo, é apresentada uma regra que faz referência a um termo de responsabilidade que determina, por sua vez, todas as responsabilidades do usuário quanto à operação adequada dos sistemas de TI da organização, conforme as políticas e normas da segurança da informação vigentes e, ainda, determina a aplicação de legislação em caso de não cumprimento.

- Planejamento de capacidade.
- Homologação.

O planejamento prévio é importante para garantir os recursos necessários aos sistemas, facilitando a sua aprovação na organização. Nesse contexto, são importantes o planejamento de capacidade e um processo adequado de homologação.

No planejamento de capacidade, atenta-se para as demandas por capacidades futuras, com o propósito de disponibilizar o poder de processamento e armazenamento adequados aos requisitos impostos. É salutar também a preocupação com as tendências em relação a aplicações e sistemas de informação, entre outros aspectos influenciadores para o contexto.

Quanto à homologação, é importante identificar previamente os critérios de aprovação e aceitação, e os testes adequados para os sistemas. Alguns critérios relevantes: desempenho, capacidade de processamento, recuperação de erros, planos de contingência e medidas de segurança adotadas. Em particular, todos os critérios e premissas considerados para a homologação devem ser definidos, acordados, documentados e testados.

Exercício de fixação 1
Procedimentos e responsabilidades operacionais

Explique a prática de segregar responsabilidades.

Explique como deve ser o planejamento de capacidade.

Proteção contra softwares maliciosos

São várias as possibilidades, como vírus, cavalos de troia, bombas lógicas etc. A proteção deve se basear na conscientização de segurança, controle de acesso e mudanças. Algumas práticas:

- Controle da conformidade com licenças.
- Controle de riscos associados a arquivos e softwares obtidos via rede.
- Instalação e atualização regular de antivírus.

Diante da variedade de softwares maliciosos existentes atualmente, é de suma importância assegurar controles em relação aos recursos de processamento da informação e softwares nas organizações. Algumas práticas podem ser aplicadas ao contexto, como o uso de softwares de detecção de códigos maliciosos, antivírus, controle de acesso rígido, um controle adequado de mudanças, proibição do uso de software não autorizado e cuidados com arquivos e softwares obtidos via rede.

Algumas verificações também são recomendadas: verificar a presença de código malicioso nos arquivos e mídias óticas ou eletrônicas transmitidos via rede, recebidos por correio eletrônico, páginas web – tanto nos servidores como nas estações de trabalho dos funcionários da organização.

Regras para a proteção contra códigos maliciosos:

- Não abrir arquivos ou executar programas anexados a e-mails sem antes verificá-los com um programa de detecção de vírus.
- Não utilizar o formato executável em arquivos compactados, já que tal formato facilita a propagação de vírus.
- Utilizar programas de computadores licenciados para uso por parte da organização, de acordo com as disposições específicas estabelecidas em contrato.

No exemplo, são apresentadas regras aplicáveis a qualquer organização, com o objetivo de estabelecer recomendações para a proteção contra códigos maliciosos e que possam, porventura, causar incidentes de segurança. Em particular, apresenta-se também uma regra para a instalação de programa, como uma medida preventiva à instalação de softwares maliciosos.

Exercício de fixação 2
Proteção contra softwares maliciosos

Cite algumas práticas que podem ser aplicadas para a proteção contra software malicioso. Dê exemplos.

Cite algumas regras que possam ser aplicadas na sua organização.

Cópias de segurança

- Medida para assegurar a integridade e a disponibilidade de ativos.
- Geração e recuperação de cópias devem ser testadas.
- Práticas recomendadas:
  - Documentar procedimentos de recuperação.
  - Definir o modo e a frequência adequados ao negócio e à segurança da informação.
  - Armazenar cópias em locais remotos.
  - Testar mídias e procedimentos de recuperação.

As cópias de segurança (backups) representam controles cujo objetivo é assegurar a integridade e a disponibilidade de ativos. Nesse contexto, deve-se atentar não apenas para a geração das cópias, mas também para que a geração seja regular e testada, e que a recuperação seja efetuada em um tempo aceitável.

São recomendadas algumas práticas para o tratamento de cópias de segurança:

- Registrar e documentar os procedimentos de recuperação a partir de cópias de segurança;
- Definir o modo (se completo ou incremental) e a frequência da geração de cópias, de acordo com a criticidade dos ativos e os requisitos de negócio e de segurança da organização;
- Armazenar as cópias em locais remotos ou distantes o suficiente para não serem afetadas por desastres ocorridos em local específico da organização;
- Identificar os níveis adequados de proteção física e ambiental das cópias;
- Aplicar testes regulares às mídias usadas na geração de cópias;
- Testar regularmente os procedimentos de recuperação.

Os backups devem manter cópias de informações essenciais ao negócio e devem ser testados regularmente para satisfazer os requisitos dos planos de continuidade de negócios.

Exercício de fixação 3
Cópias de segurança

Quais os objetivos das cópias de segurança?

Cite algumas práticas que possam ser aplicadas na sua organização.

Política de backups

- Determinada segundo a importância dos sistemas e informações.
- Estratégias podem considerar uma combinação de métodos.
- Sistemas críticos devem manter duas cópias de segurança.
- Essencial ao plano de contingência da organização.

Manter backups completos e atualizados é um elemento importante para os planos de contingência da organização, uma vez que se pode comparar sistemas e dados atuais com os backups em caso de problemas e, em seguida, efetuar a devida recuperação.

A política de backups é determinada segundo o grau de importância dos sistemas e informações para o negócio da organização; por isso, estabelece os procedimentos, os testes e a infraestrutura necessários à proteção do backup, a fim de assegurar a continuidade dos negócios em casos de desastres ou incidentes de segurança.

Em termos de estratégias, pode-se determinar backups completos ou incrementais (em um ou mais níveis), com periodicidade variável segundo a importância do sistema ou informação em questão.

Exemplos

Regras para o tratamento de cópias de segurança:

- A cada funcionário cabe efetuar, regularmente, cópias de segurança dos seus dados.
- Manter registros das cópias de segurança geradas.
- Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original.

No exemplo, são apresentadas regras aplicáveis a qualquer organização, com o objetivo de estabelecer práticas quanto à geração e manutenção de cópias de segurança.

Exercício de fixação 4
Política de backups

Como deve ser determinada a política de backup?

Tratamento de mídias e documentos

Deve-se usar procedimentos adequados para assegurar a segurança. Algumas práticas:

- Considerar a classificação da informação antes de sua manipulação.
- Controlar acessos.
- Descartar de modo seguro.
- Estabelecer regras para mídias em trânsito.

As mídias magnéticas (discos, fitas, DVDs/CDs etc.) e documentações devem ser protegidas contra ameaças por interrupção, interceptação, modificação e fabricação. Nesse sentido, algumas práticas são aplicáveis:

- Considerar a classificação da informação antes de estabelecer procedimentos e medidas de segurança para seu processamento, armazenamento e transmissão;
- Controlar o acesso ao conteúdo de mídias e documentos;
- Descartar mídias e documentos de forma segura, tendo como base procedimentos formais. Por exemplo, utilizando incineração ou trituração;
- Para mídias em trânsito, deve-se estabelecer regras claras quanto aos transportadores, embalagens, modos de entrega (em mãos, via postal etc.).

Exercício de fixação 5
Tratamento de mídias e documentos

Cite duas práticas que devem ser adotadas na sua organização para o tratamento de mídias e documentos

_____

_____

Gerência de segurança das redes

Deve-se aplicar medidas para garantir a segurança das redes. Algumas práticas:

- Segregar responsabilidades.
- Identificar os requisitos de gerenciamento de serviços de rede.
- Tratar acessos e equipamentos remotos.
- Aplicar medidas que assegurem a confidencialidade, a integridade e a disponibilidade dos recursos envolvidos.

É importante utilizar medidas adequadas para a segurança das redes nas organizações, de acordo com a política de segurança e os requisitos legais, contratuais e regulamentares. Para tanto, recomenda-se considerar as responsabilidades operacionais para com a rede e os procedimentos necessários (incluindo acessos remotos) para a coordenação de seu gerenciamento.

Algumas práticas são recomendadas para o contexto:

- Separar as responsabilidades operacionais da rede de outras operações;
- Identificar os requisitos de segurança, níveis de serviço e requisitos de gerenciamento de serviços de rede aplicáveis à organização (sejam internos ou terceirizados). Serviços de redes englobam, por exemplo, o fornecimento de conexões e soluções de segurança, tais como firewalls;
- Determinar responsabilidades e procedimentos adequados para o gerenciamento das redes e equipamentos remotos;

- Aplicar medidas de segurança para garantir a confidencialidade e a integridade dos dados em tráfego e a disponibilidade dos recursos envolvidos nas comunicações.

Exercício de fixação 6
Gerência da segurança das redes

Cite duas práticas que devem ser adotadas na sua organização para a gerência da segurança das redes.

Transferência de informações e softwares

Deve-se proteger todos os recursos envolvidos com transferências internas e externas. Algumas práticas:

- Proteção contra códigos maliciosos.
- Definir regras para o uso seguro de recursos eletrônicos.
- Estabelecer regras para transferências sem fio (wireless).
- Garantir conformidade com a legislação.
- Atribuir responsabilidades.

Deve-se garantir a segurança em quaisquer modalidades de transferência (interna ou entre a organização e terceiros) de informações e softwares. Vale ressaltar que, para o contexto, são recursos considerados pertinentes: correio eletrônico, voz, vídeo, comércio eletrônico, downloads e aquisição de software junto a fornecedores, por exemplo.

Em particular, as transferências de informações e softwares entre organizações devem ser realizadas conforme as regras de uma política formal específica (ou acordos específicos) e requisitos legais, contratuais e regulamentares vigentes.

De modo geral, as seguintes práticas podem ser consideradas:

- Proteção contra softwares maliciosos;
- Definir claramente regras para o uso de recursos eletrônicos, tais como e-mail e serviços web. Por exemplo, restringindo retransmissões de mensagens de e-mail recebidas para endereços eletrônicos externos;
- Definir procedimentos para a segurança no uso de comunicação sem fio (wireless);
- Garantir que os recursos utilizados nas transferências de informação e softwares estejam de acordo com a legislação vigente;
- Declarar claramente as responsabilidades das partes envolvidas em casos de ocorrência de incidentes de segurança.

Monitoramento

Procedimento regular para a segurança da informação em termos de operações e comunicações.

Devem ser mantidos:

- Logs de operação.
- Logs de falhas.
- Logs de auditoria.

O monitoramento das operações e comunicações deve ser uma tarefa regular e apoiada pelos dirigentes da organização, com o intuito de garantir a adequada segurança da informação com relação aos recursos operacionais e de comunicação disponíveis, e de acordo com as necessidades levantadas após a análise/avaliação de riscos de segurança da organização. É também recomendável que todos os eventos relacionados ao monitoramento sejam devidamente registrados através de logs de operação, de falhas e de auditoria, pelo menos.

Em especial, as atividades de monitoramento e registro devem ser realizadas conforme a legislação vigente. Todos os logs devem ser protegidos contra acessos não autorizados.

As práticas a seguir podem ser adotadas para a manutenção adequada dos registros:

- O log de operações deve manter informações como as atividades de operadores e administradores de sistemas, horário de inicialização e encerramento de sistemas, erros e ações corretivas aplicadas, por exemplo;
- O log de falhas deve registrar as falhas e as respectivas ações corretivas tomadas. Em particular, é relevante que existam regras claras para a manipulação de relatórios de falhas na organização

Logs de auditoria devem ser mantidos de forma a registrar as atividades dos usuários, problemas de segurança, alterações de configuração dos sistemas, todos os acessos realizados, por um período de tempo adequado às atividades de auditoria e monitoramento.

Exemplos de procedimentos com logs:

- "Não é permitido o acesso não autorizado ao e-mail de terceiros. As tentativas de acesso devem ser registradas em log, inclusive as originadas por administradores do sistema."
- "Deve ser possível reconstituir todas as atividades dos usuários a partir de logs. Os procedimentos usados para tal monitoramento devem considerar mecanismos de responsabilização claros e divulgados nos meios de comunicação internos da organização."

São exemplificados procedimentos relevantes a considerar em termos de geração de logs em determinada organização. Os exemplos podem ser considerados para organizações reais e têm o objetivo de permitir o monitoramento de operações e atividades dos usuários, em particular.

Roteiro de Atividades 6

Atividade 6.1 – Segurança da informação na gerência de operações e comunicações

Você foi designado para desempenhar as funções de gerência de operações e comunicações. Abaixo são apresentadas algumas situações em que você deverá dizer o que deve ser feito e apresentar a sua justificativa:

No	Situação	Respostas/Procedimentos	Justificativa
01	Entrada de um novo funcionário na empresa, que será usuário do sistema de controle financeiro da organização.		
02	O banco de dados foi corrompido e não havia backup.		
03	Uma máquina servidora apresentou problemas e necessita ser encaminhada para manutenção fora do ambiente do datacenter.		
04	A Gerência de Recursos Humanos informou que adquiriu um novo sistema e determinou que este deve ser instalado no servidor de aplicações que lhe atende atualmente.		
05	A Gerência de Pesquisa e Desenvolvimento avisou que a administração do servidor de aplicações, do banco de dados e do controle de versões será feita pelo mesmo pesquisador.		
06	Num levantamento realizado por uma consultoria externa para levantamento da maturidade em segurança da informação, identificou-se que vários computadores de docentes estão sem antivírus instalados.		
07	Foi identificado na divisão financeira que houve uma alteração nos arquivos, mas não foi possível identificar quem executou tal alteração.		

Atividade 6.2 – Implementando a segurança da informação na gerência de operações e comunicações de sua organização

Você ainda é integrante do comitê de segurança da informação, e deverá apresentar propostas para a segurança da informação na gerência de operações e comunicações da sua organização. Elabore para cada um dos itens a seguir cinco tópicos que devem ser abordados em cada política:

a. Cópias de segurança.

b. Procedimentos contra software malicioso.

c. Tratamento de mídias.

d. Tratamento de documentos.

e. Segurança das redes.

f. Transferência de informações.

7

Segurança de acesso e ambiental

objetivos

Descrever procedimentos e responsabilidades, e selecionar e aplicar controles e procedimentos de segurança de acesso e ambiental.

conceitos

Política de controles de acesso, controles de acesso lógico e físico, controle ambiental e segurança em Recursos Humanos.

Exercício de nivelamento 1
Segurança de acesso e ambiental

O que você entende por acesso físico?

O que você entende por acesso lógico?

Política de controle de acessos

Deve ser definida e documentada. Considerar, pelo menos:

- Informações x negócios.
- Classificação das informações.
- Requisitos para autorização.
- Análise regular dos controles.

A política de controle de acessos deve ser definida e documentada para as organizações no sentido de garantir as devidas medidas e procedimentos de segurança aos recursos lógicos e físicos, em conformidade com os requisitos do negócio. Sendo assim, a política de controle de acesso deve considerar, pelo menos:

- Informações manipuláveis por aplicações de negócios e os riscos inerentes;
- A **classificação das informações**;
- Legislação, requisitos regulamentares e contratuais vigentes pertinentes à proteção de acesso;
- Requisitos para autorização formal de pedidos de acesso e remoção de direitos;

Classificação da informação
Processo para definir a sensibilidade da informação e quem tem acesso a essa informação, permitindo assim definir níveis e critérios de acesso que garantam a segurança da informação. Vide ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação.

- Requisitos para verificação regular dos controles de acesso.

Observe que a política em questão deve contemplar, em conjunto, controles de acesso lógico e físico.

Exercício de fixação 1
Política de controle de acesso

O que deve ser considerado na política de controle de acesso?

Controles de acesso lógico

Medidas e procedimentos para a proteção de recursos computacionais, como redes, arquivos, aplicativos etc. Considerar:

- Identificação dos recursos a proteger.
- Atribuição adequada de direitos de acesso e seu devido monitoramento.
- Educação para a segurança da informação.

Em termos de controle de acesso lógico, serão vistos a seguir subtópicos que contemplam as principais preocupações e boas práticas para o contexto, além de apresentar aspectos fundamentais ao controle de acesso lógico conforme os requisitos de segurança global e de negócios das organizações.

Estude a Seção 9 da norma ABNT NBR ISO/IEC 27002:2013: Controle de acesso.

O controle de acesso lógico compreende um conjunto de medidas e procedimentos adotados pela organização ou intrínsecos aos softwares e sistemas utilizados, e visa proteger recursos computacionais e informações, de modo a assegurar:

- Que apenas usuários autorizados obtenham acesso aos recursos e que esses recursos sejam aqueles realmente necessários à execução de suas atividades;
- Que o acesso a recursos críticos seja restrito e monitorado adequadamente. Em outras palavras, pode-se considerar que o controle de acesso lógico é um processo que utiliza medidas preventivas e procedimentos específicos para que usuários ou processos acessem recursos de modo adequado.
- Ao tratar do controle de acesso, inicialmente deve-se identificar os recursos a serem protegidos. Eis alguns dos tipicamente identificados em organizações: aplicativos (códigos-fonte e objeto), arquivos de dados e de senhas, redes, utilitários, Sistemas Operacionais, arquivos de log, entre outros.

Lembre-se de que conscientizar usuários é uma tarefa importante no sentido de garantir a eficácia das medidas e dos procedimentos adotados para o controle de acesso. Sendo assim, uma boa prática é que os usuários se mantenham informados a respeito de suas responsabilidades sobre a manutenção dos controles de acesso da organização.

Funções relacionadas:

- Identificação.
- Autenticação.
- Autorização.
- Monitoramento.
- Gerência.

As funções diretamente relacionadas ao controle de acesso lógico são: identificação e autenticação, para usuários e processos, e atribuição, gerência e monitoramento de direitos de acesso, ou privilégios que indicam exatamente o grau de autorização de acesso.

- **Identificação**: todo usuário/processo que possa vir a acessar recursos computacionais deve ser identificado unicamente no ambiente, por exemplo, via login, com o objetivo de permitir um controle de ações utilizando logs;
- **Autenticação**: além da identificação, o usuário deve fornecer alguma informação complementar para provar que essa é a sua verdadeira identidade. Por exemplo, um usuário que faz um logon numa estação de trabalho informa a sua identificação (login) e uma senha – esse é o autenticador que permite que o sistema verifique se a identidade do usuário é verdadeira. Portanto, a autenticação tem por objetivo dispor um modo de verificação da identidade de usuários/processos antes de estes obterem acesso aos recursos. Sendo assim, há basicamente três modos possíveis: prova por características (físicas), prova por posse e prova por conhecimento. Por exemplo, usando reconhecimento facial ou de voz, smart cards e senhas (ou tokens), respectivamente;
- **Atribuição**: a atribuição de direitos e permissões de acesso pode ser determinada sob dois aspectos: o que um usuário/processo pode fazer ou o que pode ser feito com determinado recurso. Na primeira possibilidade, cada usuário ou recurso recebe uma permissão (ou capacidade) que, por sua vez, define todos os seus direitos de acesso a outros recursos. Na segunda, usam-se listas de controle de acesso (ou ACLs – Access Control Lists) para cada recurso, definindo, assim, os direitos de acesso de outros recursos ou usuários sobre o recurso associado a essas listas;
- **Monitoramento**: pode ser realizado através da verificação de logs, trilhas de auditoria, mecanismos de detecção de invasão, entre outros, que possam servir para tomar decisões a respeito de medidas corretivas adequadas em casos de incidentes de segurança;
- **Gerência**: responsável por aplicar medidas adequadas aos riscos inerentes a controles de acesso lógico inadequados, em função das determinações dispostas na política de segurança.

A gerência de controles de acesso lógico tem o objetivo de redução de riscos.
Considerações:

- Classificação e valor dos ativos “lógicos”.
- Necessidades reais de acesso.
- Responsabilidades dos usuários.

A gerência de controles de acesso lógico deve aplicar medidas que reduzam riscos, observando, para tanto, algumas considerações definidas na política de segurança da organização, a saber:

- Classificação dos sistemas e informações;
- Necessidades de obtenção de acesso a sistemas e dados;
- Responsabilidades dos usuários;
- Valores dos ativos;
- Demais informações relevantes para um controle de acesso lógico apropriado.

Em especial, ao tratar da gerência de controle de acesso lógico no que diz respeito à autorização, é importante considerar a manutenção adequada dos direitos de acesso a novos recursos e o uso de dispositivos móveis (notebooks, palms etc.) em função de seus riscos inerentes.

Exemplos de recomendações para o uso de senhas na gerência de controles de acesso lógico:

- "É dever da gerência de segurança desabilitar contas inativas, sem senhas ou com senhas padronizadas."
- "A senha inicial de usuários deve ser gerada de modo que já esteja expirada, forçando a entrada de uma nova senha no primeiro logon."
- "Devem ser bloqueadas contas de usuários após determinado número de tentativas de acesso sem sucesso."

Esses são exemplos de recomendações para processos de autenticação baseados em senhas e que podem ser utilizados em organizações reais.

Recomenda-se orientar os usuários no sentido de escolherem senhas mais seguras, evitando o uso de senhas muito curtas ou muito longas (aconselha-se o uso de oito caracteres) — o que pode gerar efeitos colaterais, como escrever senhas em papel; evitando, ainda, o uso de uma mesma senha para acessos a sistemas/recursos distintos. É interessante, também, o uso de geradores de senhas aleatórias, aumentando a confiabilidade dos sistemas de autenticação.

- Boas práticas:
- Atribuir direitos de acesso conforme as necessidades.
- Revisar regularmente os acessos atribuídos.
- Controlar contas e senhas.
- Manter e analisar logs regularmente.

Para a devida gestão dos controles de acesso lógico de uma organização, algumas boas práticas são recomendadas a seguir:

- Atribuir direitos de acesso aos usuários, segundo as necessidades reais de seu trabalho/cargo;
- Revisar regularmente as listas de controle de acesso e capacidades;
- Disponibilizar contas de usuários apenas a pessoas autorizadas;
- Armazenamento de senhas criptografadas;
- Manter e analisar logs e trilhas de auditoria.

Para obter detalhes sobre boas práticas no uso de senhas, consulte: https://security.web.cern.ch/security/recommendations/en/passwords.shtml e http://www.csirt.pop-mg.rnp.br/docs/senhas.pdf

Exercício de fixação 2
Controles de acesso lógico

Quais as funções diretamente relacionadas ao controle de acesso lógico?

O que deve ser considerado ao tratar da gerência de controle de acesso lógico no que diz respeito à autorização?

Cite duas boas práticas recomendadas para a gestão dos controles de acesso lógico da sua organização.

Controles de acesso físico

- Medidas preventivas e procedimentos para a proteção de recursos físicos.
- São uma barreira adicional à segurança de acesso lógico.

Estude a Seção 11 – Segurança física e do ambiente da norma ABNT NBR ISO/IEC 27002:2013.

Serão vistas, a seguir, as principais preocupações e boas práticas para o controle de acesso físico, com a apresentação de aspectos fundamentais e as influências provenientes dos requisitos de segurança global e de negócios das organizações.

Os controles de acesso físico têm o objetivo de aplicar medidas preventivas para proteger equipamentos, documentações, suprimentos e informações contra acessos não autorizados, perdas etc. Sendo assim, tais controles servem como uma barreira adicional de segurança para o controle de acesso lógico.

Considerar, ainda, o uso de áreas protegidas e perímetros de segurança. Nas áreas protegidas (com controle de acesso rígido), recomenda-se o processamento de informações críticas para o negócio da organização. Os perímetros de segurança protegem áreas que disponham de facilidades de processamento; por exemplo, um balcão de controle de acesso com registros e supervisão efetivos.

Categorias:

- Controles administrativos.
- Controles explícitos.

No tocante a controles de acesso físico, há duas categorias:

- **Controles administrativos:** compreendem medidas e procedimentos administrativos para a proteção física da organização. Em termos práticos, aconselha-se, nesse contexto, aplicar formas de identificação única de funcionários e visitantes, e até mesmo de categorias de funcionários; exigir a devolução de ativos da organização em casos de demissão de funcionários; controlar a entrada/saída de visitantes; exigir mesa limpa e organizada, entre outros;
- **Controles explícitos:** implementados através do uso de fechaduras, cadeados, câmeras de vídeo, alarmes e guardas de segurança, por exemplo.

Exemplo de recomendação para o controle de acesso físico a equipamentos:

- "O acesso a equipamentos específicos de hardware deve ser restrito a funcionários competentes, com uso registrado e baseado nas necessidades da organização."

Neste exemplo, é apresentada uma recomendação para o controle de acesso físico nas organizações, podendo ser incluída em organizações reais como item da política de controle de acesso e da política de segurança.

Gerência de controles de acesso físico:

- Identificam riscos e procuram minimizar impactos.
- Apoiada pela política de segurança da informação e política de controles de acesso.
- Deve considerar a relação custo x benefício.

A gerência de controles de acesso físico deve procurar levantar os riscos potenciais e impactos causados por incidentes originados por falhas de segurança física, aplicando medidas adequadas à organização.

Observe que, conforme expresso anteriormente, as medidas e procedimentos para controles de acesso físico devem constar na política de controles de acesso, apoiando, assim, a política de segurança da informação da organização; consequentemente, tais documentos em conjunto apoiam a gerência de controles de acesso físico.

Boas práticas:

- Uso de técnicas de identificação.
- Devolução de ativos.
- Controle de entrada e saída de visitantes.
- Vigilância 24 x 7.
- Rever e atualizar direitos de acesso.
- Manter mesa e tela limpas.

Entre as boas práticas para o adequado controle de acesso físico (e sua gerência), destacam-se:

- Usar técnicas visíveis de identificação;
- Exigência da devolução de ativos da organização quando o funcionário detentor dos mesmos for demitido ou desligado de suas funções;
- Supervisionar a entrada e saída dos visitantes, registrando data, horário de permanência e local visitado (setor, departamento etc.);
- Determinar a vigilância perene (24 x 7) na organização;
- Rever e atualizar regularmente os direitos de acesso;
- Incentivar a política da mesa limpa, entre outros.

Exercício de fixação 3
Controles de acesso físico

Qual o objetivo do controle de acesso físico?

O que são controles explícitos e controles administrativos?

Cite duas boas práticas recomendadas para a gestão dos controles de acesso físico da sua organização.

Controles ambientais

- Visam a proteção de recursos contra ameaças à disponibilidade e à integridade.
- É possível aplicar medidas preventivas e/ou corretivas.

Em termos de controle ambiental, são apresentadas algumas práticas específicas para a redução de riscos associados a ameaças no ambiente das organizações, conforme os requisitos de segurança global e de negócios.

Os controles ambientais visam proteger a organização em termos, especificamente, da disponibilidade e da integridade de seus recursos, isto é, contra desastres naturais e falhas no fornecimento ou descargas de energia elétrica, por exemplo.

Dependendo da ameaça, pode-se estabelecer medidas preventivas e/ou corretivas. A seguir, serão apresentadas boas práticas para assegurar os controles ambientais adequados.

Ameaças específicas e medidas:

- Incêndios.
- Falhas no fornecimento de energia elétrica.
- Descargas elétricas.
- Ameaças que envolvam água.
- Problemas com temperatura e ventilação.

Conforme foi visto, há várias ameaças em termos ambientais para as organizações. Eis uma lista dessas principais ameaças e das medidas respectivas a serem aplicadas para seu controle:

- **Incêndios:** aconselhável o uso de dispositivos de detecção de fumaça ou calor, a instalação de para-raios, a adoção de políticas antifumo, a disposição de um número suficiente de extintores de incêndio, a instalação de sistemas automáticos de combate ao fogo, a verificação regular de todos os dispositivos empregados contra incêndios e o treinamento de funcionários quanto a sua utilização;
- **Falhas na energia elétrica e descargas elétricas naturais:** são recomendados estabilizadores, nobreaks, geradores alternativos de energia elétrica, instalação de para-raios, desligamento de equipamentos em situação de tempestades fortes;
- **Ameaças que envolvam água**: é relevante a instalação de equipamentos em locais com baixa suscetibilidade à água, cuidados de manutenção com o telhado, rede de esgotos e encanamentos e aparelhos de ar-condicionado;
- T**emperatura e ventilação:** deve-se considerar, nesse caso, cuidados com canaletas de ventilação, circulação de ar, dispositivos que auxiliem no monitoramento da temperatura e na ventilação do ambiente e a manutenção regular dos equipamentos envolvidos.

Boas práticas:

- Planejamento de alocação dos equipamentos e móveis.
- Manutenção da limpeza e conservação.
- Implantação de dispositivos de combate ao fogo e redução do impacto de problemas com energia elétrica.
- Vistoria regular de dispositivos.

Segue uma lista de boas práticas para garantir o controle ambiental adequado nas organizações:

- Planejar a disposição de móveis e equipamentos, facilitando a circulação das pessoas;
- Manter a limpeza e a conservação do ambiente;
- Implantar sistemas de combate automático ao fogo;
- Instalar dispositivos que minimizem os efeitos de falhas no fornecimento de energia elétrica;
- Manutenção adequada de potenciais focos de problemas com água;
- Vistoriar regularmente todos os dispositivos relacionados diretamente à conservação da segurança do ambiente.

Exercício de fixação 4
Controles ambientais

Qual o objetivo dos controles ambientais?

Cite duas boas práticas recomendadas para a gestão dos controles de acesso físico da sua organização.

Segurança de Recursos Humanos

- Antes da contratação.
- Encerramento e mudança de contrato.
- Educação para a segurança da informação.

Neste tópico, serão apresentados alguns dos principais aspectos relacionados à segurança da informação nas organizações – a segurança dos Recursos Humanos, que, por sua vez, representa um dos pilares para a segurança da informação adequada e conscientizada em termos de possíveis erros humanos. Sendo assim, serão vistas algumas práticas e preocupações para o tratamento de pessoas, desde a seleção, considerando também a educação delas em termos de segurança da informação.

Acompanhe com a leitura da seção 7 – Segurança em Recursos Humanos, da norma ABNT NBR ISO/IEC 27002:2013.

Antes da contratação:

- Deixar claros papéis e responsabilidades (inclusive legais).
- Rígido processo de seleção:

Verificar referências, conhecimentos e índole.

- O contrato deve contemplar termos e condições específicas, fortalecido pelo código de conduta e termo de confidencialidade.

A seleção de candidatos deve ser rígida em função, principalmente, do cargo pretendido e de sua criticidade para os negócios. Considere que "candidato" pode representar futuro funcionário, funcionário que visa mudar de cargo ou, ainda, prestador de serviços.

Durante a seleção de pessoas, a organização deve deixar claras as responsabilidades e os papéis do candidato, em caso de contratação, perante a segurança da informação, através da apresentação de uma descrição detalhada e dos termos e condições de contratação.

Sendo assim, é importante destacar, em documentos a serem assinados pelo contratado, requisitos como agir de acordo com a política de segurança da informação e notificar superiores a respeito de eventos adversos que possam caracterizar riscos de segurança à organização.

A seleção em si, conforme dito antes, deve ser rígida o suficiente para contemplar a verificação de referências satisfatórias de caráter; a confirmação das qualificações acadêmicas e profissionais; podendo inclusive considerar verificações financeiras (de crédito) e de registros criminais. Vale ressaltar também que pode ser relevante, dependendo da situação, uma seleção rígida de fornecedores e terceiros.

Os termos e condições devem ser claramente expostos no contrato, de modo que este seja assinado indicando que o contratado concorda com suas responsabilidades perante a segurança da informação da organização (inclusive as responsabilidades legais). Neste contexto, são também convenientes a orientação para que seja seguido um código de conduta e a assinatura de um termo de confidencialidade antes da disponibilização do acesso ao contratado.

O acordo de confidencialidade deve contemplar os requisitos para proteção de informações confidenciais, considerando a legislação vigente aplicável. Em particular, seu conteúdo deve compreender, pelo menos, uma definição da informação a ser protegida, o tempo de duração do acordo, responsabilidades e ações dos envolvidos para prevenir divulgações não autorizadas, escopo de direitos dos funcionários para o uso das informações, direitos de auditoria e monitoramento, e ações específicas para casos de violação do acordo.

Encerramento e mudança de contrato:

- Exigir responsabilidades e requisitos de segurança.
- Devolver ativos.
- Retirar direitos de acesso.

Ao encerrar ou mudar o contrato de um funcionário (ou terceiro), é importante que a organização viabilize meios adequados para um processo ordenado e coordenado.

Neste contexto, algumas práticas são aplicáveis:

- No ato do desligamento de uma função, a comunicação deve informar a respeito dos requisitos de segurança e das responsabilidades legais exigidas;
- Devolução de ativos, tais como equipamentos, documentos, softwares, computadores móveis, cartões de crédito, cartões de acesso, crachás etc.;
- Retirar direitos de acesso a informações e recursos. No caso de mudanças de cargo, deve-se rever os direitos, de modo a não permitir acessos que não foram aprovados para a nova função. Se, por exemplo, o funcionário com atividades encerradas na organização tiver conhecimento a respeito de senhas de contas que permanecerão ativas após sua saída, estas devem ser alteradas.

Exercício de fixação 5
Segurança de Recursos Humanos

Durante o processo de saída da organização de um colaborador por encerramento de contrato o que deve ser realizado?

Educação para a segurança da informação:

- Promover regularmente a conscientização e treinamentos.
- Divulgar riscos, quem procurar e a quem relatar problemas.
- Deve ser uma tarefa contínua nas organizações.

Se funcionários ou terceiros não estiverem realmente conscientes em termos de suas responsabilidades e obrigações para com a segurança da informação da organização, podem ser considerados, por si só, como riscos, podendo causar impactos aos negócios.

Sendo assim, deve-se promover regularmente treinamentos, palestras e atividades de divulgação de orientações para a segurança da informação a todas as pessoas, de modo que estas conheçam os procedimentos de segurança, façam uso correto de recursos, serviços oferecidos e informações.

Nos processos de educação para a segurança da informação, é importante conscientizar as pessoas em termos dos riscos, e informá-las a quem devem relatar eventos adversos e procurar para obter orientações.

Através de iniciativas para a educação em segurança da informação, consegue-se minimizar riscos, já que as pessoas são sensibilizadas para seguir as regras da segurança da informação no seu dia a dia.

Exemplo de recomendação para a conduta de pessoas perante o uso de recursos e informações críticas:

- "A organização se reserva o direito de revogar os privilégios de usuário a qualquer sistema e a qualquer momento em função de condutas ofensivas ou prejudiciais ou, ainda, que afetem a capacidade de outras pessoas executarem suas funções adequadamente."

Neste exemplo, é apresentada uma recomendação para o tratamento de pessoas nas organizações, explicitando especialmente regras para sua conduta diante dos negócios e manipulação de recursos e informações críticas. Tal recomendação também pode ser aplicada para uma segurança eficiente de Recursos Humanos.

Roteiro de Atividades 7

Atividade 7.1 – Entendendo a segurança de acesso e a segurança ambiental

Você foi designado(a) para realizar uma avaliação da segurança de acesso e segurança ambiental de sua organização. A seguir são apresentadas algumas situações que foram encontradas e para as quais você deverá dizer o que deve ser feito e apresentar a sua justificativa para isso:

No	Situação	Respostas/Procedimentos	Justificativa
01	Funcionários sem identificação (crachá).		
02	Visitantes andando pela organização sem qualquer identificação ou registro da sua entrada.		
03	Sala de arquivo documental sem extintores ou sistema de detecção.		
04	Os colaboradores terceirizados não realizaram nenhum treinamento sobre segurança da informação.		
05	Foi identificado que ex-funcionários ainda possuíam contas de usuários de alguns sistemas.		
06	No setor de registro contábil os funcionários compartilham a mesma senha.		
07	Na área de pesquisa e desenvolvimento foi descoberto de que alguns funcionários de nível técnico possuíam acesso a áreas restritas aos pesquisadores.		

Atividade 7.2 – Políticas de acesso

1. Qual o mínimo que deve constar numa política de controle de acesso?

2. O que são controles de acesso lógico? E de acesso físico?

3. Quais são as categorias de controles de acesso físico existentes? Quais as diferenças entre elas?

4. Cite duas ameaças ambientais e seus respectivos controles ambientais.

Atividade 7.3 – Implementando a segurança de acesso e ambiental na sua organização

Você ainda é integrante do comitê de segurança da informação, deverá apresentar algumas propostas para a segurança da informação na segurança de acesso e ambiental da sua organização. Assim, elabore para cada um dos itens a seguir cinco tópicos que devem ser abordados em cada respectiva política e justifique apresentando os controles da norma que a política está atendendo:

a. Controle de acesso lógico.

b. Senhas.

c. Acesso físico.

d. Controles ambientais.

e. Segurança de Recursos Humanos.

8

Segurança organizacional

objetivos

Descrever procedimentos e responsabilidades e selecionar e aplicar controles para a segurança organizacional.

conceitos

Infraestrutura organizacional para a segurança da informação, tratamento de ativos e segurança da informação de terceiros.

Exercício de nivelamento 1
Segurança organizacional

O que você entende por segurança organizacional?

Como é feita a segurança organizacional na sua instituição?

Infraestrutura organizacional para a segurança da informação

- Importância da infraestrutura.
- Atribuição de responsabilidades.
- Coordenação da segurança da informação.

Estude a Seção 6 da norma ABNT NBR ISO/IEC 27002:2013 –Organizando a segurança da informação.

Neste tópico serão apresentados os aspectos relevantes para o estabelecimento de uma infraestrutura de apoio à segurança da informação nas organizações. Em especial serão tratadas a razão da importância da infraestrutura, a relevância da atribuição de responsabilidades e questões relacionadas à coordenação.

Importância da infraestrutura

Fornece todas as condições para a gestão da segurança da informação na organização. Uma recomendação é definir uma estrutura de gerenciamento para controlar a elaboração e implantação da segurança da informação.

Para garantir a segurança da informação em determinada organização, deve-se atentar para a necessidade do estabelecimento de uma infraestrutura que propicie o seu gerenciamento. Inicialmente, é válido definir uma estrutura de gerenciamento própria para o controle da implantação da segurança da informação.

Em particular, se for o caso, é relevante a contratação de consultoria especializada com o propósito de elaborá-la e implantá-la na organização.

Atribuição de responsabilidades

- Deve-se atribuir responsabilidades de acordo com a política de segurança.
- Funcionários podem delegar tarefas de segurança da informação, mas não podem delegar responsabilidades.
- Se necessário, é preciso instituir o cargo de gestor de segurança da informação.
  Preocupações:
- Áreas de responsabilidade.
- Responsabilidades dos funcionários.
- Processos a serem implementados.

Atribuir responsabilidades é uma atividade considerada crucial para a segurança da informação, devendo ser realizada de acordo com a política de segurança da informação da organização.

Funcionários (ou pessoas em determinados cargos) que possuam responsabilidades definidas formalmente na política de segurança podem delegar atividades relacionadas diretamente à segurança da informação, todavia, não se eximindo das responsabilidades. Sendo assim, é relevante que, nos casos de delegação, os funcionários que delegam a atividade avaliem se esta está sendo realizada conforme a política de segurança, legislação e normas vigentes.

Para cada ativo e procedimento de segurança da informação, é importante atribuir responsabilidades a um funcionário (ou cargo). Em outras palavras, o funcionário (ou cargo) deverá efetuar a gestão do ativo ou procedimento segundo determinação da política de segurança.

Dependendo do tamanho e das vulnerabilidades da organização, pode-se estabelecer o cargo de gestor da segurança da informação, que responde, em primeira instância, pela segurança global da organização e ainda auxilia no desenvolvimento da política de segurança e define a estratégia para a sua divulgação, exigindo seu cumprimento por todos. Ao gestor, cabe estar sempre atualizado em relação aos problemas, riscos e soluções de segurança; selecionar os mecanismos de segurança mais adequados aos problemas de segurança específicos da organização; e verificar a adequação da política de segurança, mecanismos e procedimentos de segurança da informação adotados.

Exercício de fixação 1
Atribuição de responsabilidades

Que atribuições devem ser atribuídas ao gestor da segurança da informação?

Por que a atribuição de responsabilidades é uma atividade crucial para a segurança da informação?

Coordenação da segurança da informação

Compreende a colaboração entre partes, como dirigentes, funcionários, auditores, consultores etc. Objetivos:

- Aprovar metodologias e procedimentos de segurança da informação.
- Assegurar a conformidade com a política de segurança.
- Coordenar a implantação de controles.
- Educar para a segurança da informação.

Para a efetividade da segurança da informação em uma organização, seus dirigentes devem montar uma equipe multidisciplinar (dirigentes e funcionários de vários departamentos, por exemplo) para coordenar as atividades necessárias. Se necessário, pode-se também instituir um comitê específico.

Em particular, recomenda-se que a coordenação atue nas seguintes atividades:

- Avaliar e aprovar metodologias e procedimentos necessários à segurança da informação;
- Controlar todos os procedimentos, com o intuito de assegurar a conformidade com a política de segurança da organização;
- Coordenar a implantação de controles de segurança da informação, tais como medidas contra acessos não autorizados;
- Divulgar adequadamente para toda a organização os procedimentos, os controles e a política de segurança. Lembre-se sempre de que a conscientização das pessoas pode ser considerada tão relevante quanto o uso de outros mecanismos de segurança baseados em tecnologia.

Exercício de fixação 2
Coordenação da segurança da informação

Em que atividades o comitê deve atuar?

Tratamento de ativos

- Proteção de ativos.
- Inventário de ativos.
- Proprietário de ativo.

Estude a Seção 8 da norma ABNT NBR ISO/IEC 27002:2013 – Gestão de ativos.

Uma vez que os ativos são elementos essenciais para o negócio das organizações, este tópico apresenta os aspectos primordiais a serem considerados. Serão apresentadas as preocupações com a proteção dos ativos e dos procedimentos recomendados, para fins de gestão de ativos e recuperação após desastres: inventário e designação de proprietário para cada ativo da organização.

Proteção dos ativos

- Ativos são elementos essenciais ao negócio da organização.
- Ativos devem ser inventariados.
- Todo ativo deve ter um responsável por manter sua segurança.

Os ativos da organização são elementos importantes para o negócio; sendo assim, sua proteção adequada deve ser estabelecida e mantida. Exemplos:

- Equipamentos;
- Bases de dados;
- Serviços de iluminação;
- Acordos;
- Procedimentos de suporte técnico;
- Trilhas de auditoria;
- Aplicativos;
- Sistemas de informação;
- Pessoas;
- Imagem comercial da organização.

Para tal proteção, são recomendados dois procedimentos: inventariar os ativos e associar a cada um deles um proprietário, responsável pela manutenção de sua segurança.

A seguir, serão apresentados mais detalhes a respeito de cada procedimento.

Exercício de fixação 3
Proteção dos ativos

O que são ativos?

_____

_____

_____

Inventário de ativos

O inventário é essencial para recuperação após desastres e compreende:

- Identificar ativos.
- Catalogar ativos.
- Manter o catálogo.

No inventário de ativos, deve-se estruturar e manter os ativos devidamente identificados. Na identificação, as informações relevantes tipicamente são: o tipo do ativo, configuração, sua criticidade para os negócios da organização, localização, informações sobre o tratamento de backups e licenças. Ainda no inventário, deve-se identificar o proprietário de cada ativo e a classificação da informação, quando cabível.

Em casos de recuperação após desastres, o inventário de ativos representa um dos itens essenciais para sua efetividade. E, para a gestão de riscos, o inventário é uma premissa.

Exercício de fixação 4
Inventário de ativos

Quais informações devem constar no inventário de ativos?

Proprietário de ativo

Aquele que é o responsável autorizado sobre o(s) ativo(s).

- Proprietário não é dono do ativo!

Atividades:

- Garantir a classificação dos ativos.
- Definir e analisar, periodicamente, as restrições de acesso aos ativos.

O proprietário de um ativo é o responsável pela manutenção da sua segurança, efetuando, então, atividades como:

- Garantir a classificação adequada dos ativos;
- Definir e analisar, periodicamente, as restrições de acesso ao ativo.

São exemplos de proprietários de ativos o gerente de RH (Recursos Humanos) da organização, responsável por documentos específicos, e o desenvolvedor responsável por sua estação de trabalho. Vale ressaltar que, se necessário e cabível, pode-se atribuir ao gestor da segurança da informação a responsabilidade por determinados ativos, principalmente aqueles diretamente relacionados à segurança da informação, como a própria política de segurança.

Exemplo: Inventário do ativo “base de dados”.

- Tipo: dados.
- Criticidade para os negócios: alta.
- Localização: sala de servidores da organização.
- Tratamento de backup: incremental e diário.
- Proprietário: administrador do banco de dados.

Este exemplo apresenta algumas informações a respeito do ativo “base de dados” de uma organização. Pode-se observar que:

- O tipo considerado é “dados”. A classificação de ativos pode variar de uma organização para outra; todavia, tipicamente pode-se categorizar em hardware, software, dados, documentação etc.;
- A criticidade do ativo é considerada alta, visto que os dados são essenciais ao negócio da organização. Pode-se associar a criticidade atribuída segundo as categorias utilizadas na análise/avaliação de riscos para a organização. Para exemplificar, pode-se classificar ativos como de alta, moderada ou baixa criticidade;
- A localização do ativo é a sala de servidores da organização, visto que se trata de uma base de dados armazenada em um banco de dados;

- O tratamento de backup aplicado ao ativo é incremental e diário. Para todos os ativos é relevante indicar a política de backup para fins de gestão de incidentes, em particular. Para fins de conhecimento, a política pode determinar, de acordo com o grau de criticidade do ativo, o backup completo ou incremental e seu período (mensal, quinzenal, semanal ou diário, por exemplo).

Por fim, indica-se o responsável pela segurança do ativo. No caso, o administrador do banco de dados da organização.

Exercício de fixação 5
Proprietário do ativo

Qual é a responsabilidade do proprietário do ativo?

Cite atividades que devem ser realizadas pelo proprietário do ativo.

Segurança da informação e terceiros

- A razão do tratamento diferenciado.
- Possíveis riscos.
- Tratamento dos clientes.
- Acordos específicos.
- Gerência de serviços de terceiros.

É relevante estabelecer procedimentos adequados antes de disponibilizar acessos por parte de terceiros. Neste tópico, serão tratados o porquê do tratamento diferenciado dos terceiros e possíveis riscos envolvidos; como tratar com os clientes a respeito da manutenção de acordos específicos para o contexto e os procedimentos recomendados para a gerência de serviços terceirizados.

Estude a Seção 15 da norma ABNT NBR ISO/IEC 27002:2013 – Relacionamento na cadeia de suprimento.

A razão do tratamento diferenciado

Deve-se manter a segurança de recursos e informações acessíveis a terceiros.

- Acessíveis = processados, transmitidos ou gerenciados.

Considerar:

- Possíveis riscos.
- Acordos específicos.

Deve-se considerar um tratamento diferenciado para os recursos e informações que sejam processados, transmitidos ou gerenciados por partes externas, por exemplo, empresas prestadoras de serviço, com o objetivo de permitir tais acessos em conformidade com a política de segurança da informação vigente na organização.

Para tanto, é relevante efetuar uma análise dos potenciais riscos envolvidos e as possíveis medidas de segurança adequadas ao tratar com partes externas. Em especial, as medidas

de segurança e demais critérios específicos quanto à segurança da informação devem ser definidos em acordo entre as partes.

Possíveis riscos

É preciso identificar, analisar e avaliar os riscos, e implementar medidas de segurança antes de disponibilizar o acesso a terceiros. Devem ser considerados:

- Recursos de processamento.
- Valor da informação.
- Pessoas envolvidas.
- Práticas e procedimentos para o tratamento de incidentes de segurança.
- Requisitos legais, regulamentares e contratuais.

No tratamento da segurança da informação em relação a terceiros, há potenciais riscos específicos. Sendo assim, é importante analisar e avaliar os riscos envolvidos diretamente com os acessos externos, aplicando as medidas de segurança adequadas antes de disponibilizar o acesso.

A seguir, são apresentados alguns dos principais aspectos a considerar para o contexto:

- Identificar os recursos aos quais terceiros podem ter acesso;
- Indicar o tipo de acesso a cada recurso;
- Conhecer o valor e a criticidade das informações disponibilizadas a terceiros;
- Aplicar medidas de segurança condizentes aos riscos para cada informação acessada por terceiros;
- Considerar as pessoas que poderão acessar a informação no lado dos terceiros;
- Implantar práticas e procedimentos para o tratamento de incidentes de segurança;
- Considerar os requisitos legais, contratuais e regulamentares aplicáveis ao contexto.

Exemplo de regras para tratamento de terceiros:

- "Não é permitida a revelação de identificação, autenticação e autorização deuso pessoal ou uso de recursos autorizados por intermédio de tais itens por parte de terceiros."
- "Não é permitido o fornecimento de informações a terceiros a respeito dos serviços disponibilizados na organização, exceto os de natureza pública ou mediante autorização de equipe/gestor competente."

Neste exemplo, são apresentadas regras de tratamento das informações e serviços por parte de terceiros, cujo objetivo é demonstrar a aplicação de procedimentos formais com vistas à segurança da informação.

Exercício de fixação 6
Possíveis riscos

Quais aspectos devem ser considerados em relação à segurança da informação de terceiros?

Tratamento dos clientes

Deve-se identificar todos os requisitos de segurança antes de disponibilizar o acesso aos clientes. Preocupações:

- Proteção dos ativos.
- Descrição detalhada do produto/serviço a ser fornecido.
- Políticas de controle de acesso.
- Responsabilidades legais.

Ao tratar com clientes, a organização deve identificar, antecipadamente, todos os requisitos de segurança diretamente relacionados ao acesso externo a ativos e informações.
Sendo assim, recomenda-se:

- Proteger os ativos, usando mecanismos de segurança adequados e indicar ações corretivas a serem aplicadas nos casos de comprometimento;
- Descrever, em detalhes, o produto/serviço a ser fornecido;
- Considerar as políticas de controle de acesso vigentes;
- Indicar as responsabilidades legais da organização e do cliente.

Acordos específicos

Deve-se considerar a segurança da informação ao estabelecer acordos com terceiros.

Considerar, pelo menos:

- Política de segurança.
- Medidas de segurança aplicadas ao ativo envolvido.
- Treinamento de funcionários.
- Atribuição de responsabilidades.
- Processo para gestão de mudanças.
- Classificação da informação disponibilizada.

Nos acordos, os requisitos de segurança devem ser contemplados a fim de assegurar o conhecimento e cumprimento deles por parte de terceiros.

Essencialmente, recomenda-se considerar, nos acordos, os seguintes aspectos:

- A política de segurança da informação vigente;
- O uso de medidas de segurança para a proteção de ativos;
- Treinamento e conscientização das pessoas em termos da segurança da informação e suas responsabilidades;
- Processo claro de gerência de mudanças;
- Políticas de controle de acesso;
- Direito de efetuar auditoria;
- Requisitos para a continuidade de serviços;
- Responsabilidades legais, contratuais e regulamentares aplicáveis.

Inclusive, podem ser definidos acordos de confidencialidade, de modo que os requisitos de segurança contemplados expressem as necessidades da organização quanto ao valor das informações para o negócio. Esses acordos protegem a informação, ao passo que determinam as responsabilidades dos envolvidos quanto à proteção, uso e divulgação das informações da organização. Sendo assim, os acordos de confidencialidade podem ser estabelecidos entre a organização e terceiros, e entre a organização e seus funcionários.

Em organizações nas quais a gestão da segurança da informação for terceirizada, os acordos devem estabelecer detalhes a respeito do modo como os terceiros garantirão a segurança atendendo a obrigações legais e aos requisitos do negócio.

Gerência de serviços de terceiros

Serviços disponibilizados e acordos com terceiros devem ser monitorados.
Boas práticas:

- Considerar a segurança da informação ao elaborar acordos de entrega de serviços.
- Disponibilizar soluções técnicas para monitoramento.
- Monitorar e analisar serviços entregues e logs.
- Gerenciar mudanças nos serviços.

Os serviços terceirizados em determinada organização devem ser gerenciados com o propósito de garantir adequação aos requisitos de segurança da informação e aos negócios. Sendo assim, os acordos estabelecidos entre a organização e terceiros devem ser gerenciados e controlados adequadamente. Práticas apropriadas:

- Deve-se considerar medidas de segurança, níveis de serviço e requisitos de entrega de serviços ao elaborar os acordos de entrega de serviços terceirizados. Tais acordos devem ser verificados para que os requisitos de segurança acordados sejam cumpridos;
- É relevante dispor de soluções técnicas e recursos suficientes para monitorar os acordos e requisitos de segurança estabelecidos;
- Deve-se monitorar e analisar regularmente serviços e logs fornecidos por terceiros;
- Deve-se gerenciar as mudanças em termos de serviços terceirizados, considerando melhorias possíveis, atualizações de políticas, estabelecimento de novos controles de segurança e uso de novas tecnologias, por exemplo.

- Exemplo:
  - Cláusula contratual – Segurança da informação.
    "A CONTRATADA obriga-se a utilizar programas de proteção e segurança da informação que busquem evitar qualquer acesso não autorizado aos seus sistemas, seja em relação aos que eventualmente estejam sob sua responsabilidade direta, seja através de link com os demais sistemas da CONTRATANTE ou, ainda, por utilização de e-mail."

Roteiro de Atividades 8

Atividade 8.1 – Entendendo a segurança organizacional

1. Explique a importância da atribuição de responsabilidades para a segurança da informação na sua organização.

2. Como e onde deve atuar a Coordenação da Segurança da Informação?

Atividade 8.2 – Realizando a segurança organizacional

1. Descreva como deve ser tratado e executado o inventário dos ativos.

2. Explique a razão do tratamento diferenciado de recursos e informações acessíveis a terceiros. Apresente um exemplo prático da sua organização.

3. Descreva os procedimentos que devem ser adotados no tratamento dos clientes.

4. Cite dois exemplos práticos para a gerência de serviços de terceiros.

Atividade 8.3 – Implementando a segurança organizacional

Você ainda é integrante do comitê de segurança da informação e deverá apresentar algumas propostas para a segurança da informação na segurança organizacional da sua organização. Assim, elabore para cada um dos itens abaixo cinco tópicos que devem ser abordados em cada política:

a. Ativos.

b. Terceiros prestadores de serviços na área de TI.

c. Terceiros prestadores de serviços na área de serviços gerais.

d. Terceiros prestadores de serviços na área de TI.

e. Fornecedores de material de escritório.

f. Clientes.

g. Acordos.

h. Responsabilidades na segurança da informação.

9

Gestão de continuidade de negócios

objetivos

Identificar os requisitos e organizar a continuidade de negócios; identificar e selecionar os procedimentos da gestão de incidentes de segurança.

conceitos

Gestão da continuidade de negócios, segurança da informação e continuidade de negócios, plano de continuidade de negócios e gestão de incidentes.

Exercício de nivelamento 1
Gestão de continuidade de negócios

O que você entende por continuidade de negócios?

Como é feita a continuidade de negócios na sua instituição?

Continuidade de negócios

- Dependência de tecnologia e sistemas computacionais.
- Impactos diversos.
- É preciso considerar:
  - Medidas de recuperação de desastres.
  - Plano de contingências.
  - Plano de continuidade de negócios.
- Preocupação dos dirigentes deve ser constante.

Estude a seção 17 – Aspectos da segurança da informação na gestão da continuidade do negócio da norma ABNT NBR ISO/IEC 27002:2013..

Neste tópico, serão vistos aspectos consideráveis para a continuidade de negócios, bem como para a sua gestão.

Hoje, as organizações são dependentes da tecnologia e dos sistemas computacionais. Assim, perdas de equipamentos e informações podem impactar o negócio da organização, causando perdas financeiras, de mercado e, até mesmo, dependendo da gravidade das ameaças, provocando sua dissolução.

Nesse contexto, são mais que necessárias a conscientização a respeito da necessidade de recuperação de desastres e o plano de contingência – ambos estratégicos para atender aos objetivos de negócio da organização. Em adição, é relevante, ainda, um plano de continuidade de negócios.

Vale ressaltar que os dirigentes da organização são responsáveis por analisar seus recursos e informações, de modo a identificar a importância de cada um deles para a continuidade dos negócios.

O plano de continuidade de negócios é de responsabilidade dos dirigentes da organização. A equipe de gerência da segurança pode auxiliar nessa tarefa, mas não pode ser responsabilizada por sua inteira implementação. Tal auxílio pode contemplar a criação, manutenção, divulgação e coordenação do plano de contingências.

Gestão da continuidade de negócios

- Combina medidas de prevenção e recuperação.
- Aspectos relevantes:
  - Identificar os processos críticos de negócios.
  - Integrar a gestão da segurança da informação.
- O plano de continuidade de negócios deve ser implementado.

A gestão da continuidade de negócios combina medidas de prevenção e recuperação, com o objetivo de impedir a indisponibilidade de serviços e atividades do negócio, protegendo, assim, os processos críticos contra impactos causados por falhas ou desastres e, no caso de perdas, prover a recuperação dos ativos envolvidos e restabelecer o funcionamento normal da organização em um intervalo de tempo aceitável. Em particular, é imprescindível identificar os processos críticos na organização e, em seguida, integrar a gestão da segurança da informação em função das exigências da gestão da continuidade de negócios.

Alguns exemplos de processos críticos são as operações gerais, tratamento dos funcionários, materiais, transporte e instalações – considerando, para o contexto, seus requisitos específicos de continuidade. Sendo assim, é importante implementar um plano de continuidade de negócios com vistas à recuperação dos processos críticos, dentro do intervalo de tempo aceitável ao negócio em caso de desastres. Vale salientar que o plano de continuidade de negócios é global para a organização, mas a segurança da informação deve ser considerada como um de seus componentes.

Para obter mais detalhes a respeito da continuidade de negócios, consulte as normas:

- ABNT NBR 15999-1:2007 Errata 1:2008 – Gestão de continuidade de negócios – Parte 1: Código de prática;
- ABNT NBR ISO 22301:2013 Segurança da sociedade – Sistema de gestão de continuidade de negócios – Requisitos.

Exercício de fixação 1
Gestão da continuidade de negócios

Qual o objetivo da gestão da continuidade de negócios?

Quais os processos críticos da sua instituição?

Segurança da informação e gestão da continuidade de negócios

A segurança da informação é estratégica. Considerações:

- Compreensão dos riscos.
- Identificação dos processos e ativos críticos.
- Compreensão dos impactos.
- Contratos de seguro.
- Identificação de medidas aplicáveis.
- Identificação dos recursos requeridos.
- Proteção de recursos de processamento.
- Documentação detalhada.
- Testes e manutenção dos planos.

Neste tópico, serão apresentadas as principais considerações para a integração da segurança da informação à gestão da continuidade de negócios. Em especial, tratando da análise de riscos e sua importância para ambos.

A segurança da informação deve ser contemplada como um item estratégico a considerar para a continuidade de negócios de uma organização. Sendo assim, ao tratar a inclusão da segurança da informação no contexto específico, as seguintes considerações devem ser atendidas:

- Compreensão dos riscos à organização em termos de probabilidades e impactos;
- Identificação dos processos críticos do negócio e dos ativos diretamente relacionados;
- Compreensão dos impactos gerados por incidentes de segurança aos negócios;
- Identificação de contratos de seguro estabelecidos para os ativos críticos da organização;
- Identificação das medidas preventivas, corretivas e orientadoras aplicáveis;
- Identificação dos recursos financeiros, de infraestrutura, técnicos e ambientais necessários para o levantamento dos requisitos de segurança;
- Consideração a respeito das medidas relacionadas à segurança de Recursos Humanos;
- Consideração a respeito das medidas que asseguram a proteção de recursos de processamento;
- Documentação detalhada sobre os requisitos de segurança da informação a serem incluídos;
- Formalização de testes e da manutenção dos planos (de continuidade de negócios e de contingências, por exemplo).

Exemplo de questão a ser considerada no plano de continuidade de negócios:

- "Perda da capacidade de proteção, processamento e recuperação das informações manipuladas nos computadores da organização, podendo ocasionar problemas na realização de seus negócios e no cumprimento de metas previamente estabelecidas em contrato com seus clientes."

O exemplo apresenta um problema a ser tratado no plano de continuidade de negócios das organizações.

Exercício de fixação 2
Segurança da informação e gestão da continuidade de negócios

Segundo o ambiente da sua organização, qual a importância da compreensão dos impactos gerados por incidentes de segurança aos negócios?

Análise de riscos e continuidade de negócios

Compreende:

- Identificar eventos adversos.
- Analisar riscos (de toda a espécie).

Em função dos resultados da análise, deve-se elaborar um planejamento de estratégias para a continuidade de negócios.

A gestão da continuidade do negócio deve começar pela identificação dos eventos adversos (identificação das possíveis ameaças), seguida de uma análise de riscos – não apenas de segurança, mas de todos os processos de negócio –, com o intuito de determinar o impacto das interrupções, tanto em relação à escala de dano causado quanto ao período de recuperação. Ambas as atividades devem ser executadas com o total envolvimento dos responsáveis pelos processos e recursos do negócio.

Dependendo dos resultados da análise de riscos, um planejamento específico deve ser desenvolvido para determinar a estratégia a ser usada para alcançar a continuidade de negócios. Nessa estratégia, deve-se determinar, por exemplo, o intervalo de tempo aceitável para recuperação dos sistemas críticos.

Com isso, há condições de decidir como e onde investir em medidas de segurança, protegendo os ativos e mantendo as atividades dentro de sua maior normalidade. Uma vez desenvolvido o plano, ele deve ser validado e implementado pelos dirigentes da organização.

Exercício de fixação 3
Análise de riscos e continuidade de negócios

Qual a finalidade da realização de uma análise de risco na gestão da continuidade de negócios?

Plano de continuidade de negócios

- Estrutura.
- Desenvolvimento e implementação.
- Testes.
- Manutenção e reavaliação.

Neste tópico, serão mostradas as fases de implementação de um plano de continuidade de negócios tipicamente propostas para organizações reais, de modo a considerar todos os requisitos de segurança da informação para a continuidade dos negócios.

Estrutura

Contemplar, pelo menos:

- Responsabilidades individuais requeridas.
- Indicação de gestor.
- Condições para acionamento.
- Procedimentos para operação temporária durante recuperação.
- Procedimentos emergenciais.
- Procedimentos de recuperação.
- Especificação do cronograma de testes e manutenção.
- Treinamentos.

A estrutura de um plano de continuidade de negócios normalmente deve contemplar:

- As responsabilidades individuais requeridas para cada uma das atividades propostas no plano;
- Indicação de um gestor específico;
- As condições necessárias para acionamento do plano; por exemplo, como avaliar o evento adverso, a quem notificar etc;
- Procedimentos que assegurem a operação temporária dos processos e sistemas de negócio enquanto a recuperação estiver em execução;
- Procedimentos emergenciais para as situações nas quais há incidentes que impactam diretamente os negócios;
- Procedimentos de recuperação de processos e operações de negócio em um intervalo de tempo aceitável;
- Especificação do cronograma de manutenção e testes do plano;
- Promoção de treinamentos a respeito da continuidade de negócios.

Como premissa, destaca-se a necessidade de os ativos e recursos críticos estarem aptos a desempenhar os procedimentos emergenciais e de recuperação propostos no plano.

Desenvolvimento e implementação

Considerar, pelo menos:

- Identificação das responsabilidades e procedimentos.
- Identificação do grau aceitável de perdas.
- Implantação dos procedimentos de recuperação.
- Conscientização quanto às responsabilidades.
- Testes.
- Manutenção regular.
- Cópias do plano em locais distintos.

Durante o planejamento da continuidade de negócios, alguns itens são determinantes e indicam o conteúdo a ser incluído no plano com vistas também à segurança da informação:

- Identificação das responsabilidades e procedimentos relativos à continuidade de negócios;
- Identificação do grau aceitável de perdas de informações e serviços;
- Implantação dos procedimentos destinados à recuperação das operações de negócio e da disponibilidade da informação, considerando o intervalo de tempo aceitável para o restabelecimento do funcionamento normal das operações;
- Conscientização das pessoas em termos de suas responsabilidades e conhecimento dos procedimentos envolvidos;
- Testes;
- Manutenção regular do plano, objetivando refletir mudanças significativas nos negócios da organização.

É relevante considerar todas as dependências externas ao negócio e contratos existentes, em especial, no que diz respeito à legislação específica aplicável. Recomenda-se, ainda, que sejam mantidas (atualizadas e protegidas) cópias do plano de continuidade de negócios em ambientes remotos, como uma medida de contingência para situações de desastres.

Exercício de fixação 4
Desenvolvimento e implementação

No ambiente da sua organização, cite três itens que são determinantes durante o planejamento da continuidade de negócios.

Testes

O plano de testes indica como e quando cada componente do plano deve ser testado. Técnicas possíveis:

- Testes de cenários.
- Simulações.
- Teste de recuperação técnica.
- Teste de recuperação em local alternativo.
- Testes de facilidade de fornecedores e serviços.
- Ensaio completo.

O plano de continuidade de negócios deve ser testado regularmente como forma de assegurar sua atualização e eficiência. Os testes devem garantir também que todos os integrantes da equipe de recuperação e outros funcionários relevantes possuem conhecimento dos planos.

Os testes devem indicar como e quando cada um de seus componentes deve ser testado. É recomendável testar os componentes individuais dos planos frequentemente. Várias técnicas podem ser utilizadas de modo a garantir a exatidão com a qual os planos operarão na vida real. Entre elas, destacam-se:

- Teste de vários cenários (discutindo os acordos de recuperação, por exemplo, usando interrupções);

- Simulações (particularmente úteis para o treinamento de pessoal em seus postos e funções de gerenciamento de crise);
- Teste de recuperação técnica (assegurando que os sistemas de informação podem ser efetivamente recuperados);
- Teste de recuperação em um local alternativo (executando os processos do negócio em paralelo com as operações de recuperação fora do local principal);
- Testes de facilidades de fornecedores e serviços (garantindo que os serviços e produtos fornecidos por fontes externas satisfazem os requisitos contratados);
- Ensaio completo (testando a organização, o pessoal envolvido, os equipamentos, as facilidades de processamento e os processos para confirmar que podem enfrentar e superar interrupções do ambiente operacional).

Manutenção e reavaliação

- Manutenção regular.
- Atualizar o plano em virtude de mudanças.
  - Nos negócios (objetivos e/ou estratégias).
  - Aquisição de novos equipamentos e sistemas.
  - Legislação.
- Deve-se estabelecer responsabilidades para reavaliações regulares.

O plano de continuidade de negócios deve passar por uma manutenção em intervalos regulares de tempo e ser atualizado de forma a garantir sua efetividade. Além de mudanças nos negócios, entre outras, apresentadas a seguir, que possam indicar necessidades de melhorias do plano, os testes realizados devem ser devidamente documentados e servir como fonte de dados para atualizações.

Mudanças relevantes a serem consideradas na manutenção do plano compreendem a aquisição de novos equipamentos, de novos sistemas (ou a atualização destes), mudanças de estratégias de negócio e mudanças na legislação.

É recomendável estabelecer a responsabilidade para as revisões regulares. A identificação das modificações já ocorridas no negócio, mas ainda não incluídas no plano, é um sinal de que há necessidade de manutenção. O processo de controle de mudança deve garantir que os planos atualizados serão distribuídos pelos setores responsáveis (e para o local remoto, de modo adequado).

Exemplo de recomendação para a continuidade de negócios – Comprometimento do ambiente de TI:

- "Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas. Nesses casos, uma versão segura do Sistema Operacional, assim como dos softwares de segurança, deverá ser baixada novamente, e as alterações recentes de usuários e privilégios do sistema devem ser revisadas a fim de detectar modificações não autorizadas de dados."

O exemplo apresenta procedimentos recomendados para serem acionados devido à ocorrência de desastres no ambiente de TI, visando a continuidade de negócios.

Exemplo de diretriz para a conscientização em segurança da informação e continuidade de negócios:

- "A divulgação das regras, riscos, procedimentos e políticas de segurança aos usuários finais deve ser objeto de campanhas internas permanentes, seminários de conscientização e quaisquer outros meios ou iniciativas para a consolidação da educação para a segurança da informação."

A diretriz mostrada no exemplo compreende diretamente as preocupações com a educação para a segurança da informação e, por consequência, auxilia no sentido de garantir a continuidade de negócios da organização.

O DSIC publicou a Norma Complementar 06/IN01/DSIC/GSIPR – Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações, que aborda o tema de continuidade de negócios para os órgãos da Administração Pública Federal (APF).

Exercício de nivelamento 2
Gestão de incidentes de segurança

O que você entende por continuidade de negócios?

Como é feita a continuidade de negócios na sua instituição?

- Notificação de eventos adversos.
- Procedimentos da gestão de incidentes de segurança.
- Definição de responsabilidades e procedimentos efetivos.
- Aplicar medidas corretivas após notificação.
- Monitoramento regular é apropriado como medida de detecção.

Neste tópico, serão apresentados alguns dos principais aspectos relacionados à segurança da informação nas organizações – a gestão de incidentes de segurança, apresentando, assim, as preocupações relativas à notificação de incidentes e aos procedimentos necessários à sua gestão.

Estude a seção 16 – Gestão de incidentes de segurança da informação da norma ABNT NBR ISO/IEC 27002:2013.

A gestão de incidentes de segurança da informação engloba a definição de responsabilidades e procedimentos efetivos para o controle de eventos adversos (incidentes) após a notificação. Sendo assim, a gestão de incidentes envolve procedimentos para a notificação de eventos adversos de segurança e aplicação de medidas adequadas para sua resolução. Vale observar que, além da notificação, é importante um efetivo monitoramento da organização como medida de detecção de incidentes de segurança.

Notificação de eventos adversos

- Efetuada para acionar as medidas adequadas em tempo aceitável.
- As pessoas devem ser conscientizadas a respeito dos procedimentos de notificação.
- As notificações devem ser emitidas aos responsáveis diretos pela gestão de incidentes.

Uma série de eventos adversos (ou incidentes de segurança) pode ocorrer nas organizações, como, por exemplo, perdas de equipamentos e recursos; sobrecarga de sistemas; violações de controles de acesso físico/lógico; mau funcionamento de hardware/software, códigos maliciosos, negação de serviço (DoS – Denial of Service), uso impróprio de sistemas de informação, entre outros.

A notificação de eventos adversos deve ser efetuada para que a ação corretiva adequada seja aplicada em tempo hábil. Nesse sentido, é importante que todas as pessoas (funcionários, terceiros etc.) sejam informadas a respeito dos procedimentos formais necessários para a notificação e que, assim, se tornem responsáveis por notificar qualquer evento adverso ou vulnerabilidade que possa causar impacto à segurança da informação da organização.

Vale salientar que as notificações devem ser emitidas para o responsável (pessoa ou equipe) direto por recebê-las na organização. Com isso, é importante identificar quem é o responsável antecipadamente e de modo formal. Além disso, pode-se utilizar ferramentas como formulários específicos para auxiliar as pessoas na preparação da notificação e, ainda, registrar o evento adverso.

Exercício de fixação 5
Notificação de eventos adversos

Qual a finalidade da notificação de eventos adversos?

Procedimentos da gestão de incidentes de segurança

Ações efetivas, rápidas e ordenadas. Compreendem:

- Planos de contingências.
- Identificação e análise da causa do incidente.
- Planejamento e implementação de medidas corretivas.

Para a gestão de incidentes de segurança, é preciso estabelecer procedimentos adequados a serem seguidos após sua notificação. Nesses procedimentos, devem constar as ações efetivas a serem tomadas de modo ordenado e rápido.

Os procedimentos de gestão de incidentes de segurança devem contemplar:

- Planos de contingência;
- Identificação e análise da causa do incidente de segurança. A análise, em particular, deve fornecer informações a respeito dos tipos, quantidades e custos relativos aos incidentes de segurança de modo a dar uma ideia do impacto de sua ocorrência para a organização (negócios, principalmente) e, por consequência, dar indícios a respeito das necessidades quanto à ação a ser tomada;
- Planejamento e implementação de uma ação corretiva que evite a repetição do incidente.

Uma questão relevante deve ser considerada: manter procedimentos que determinem quem contatar e quando contatar em casos de incidentes que envolvam autoridades como, por exemplo, corpo de bombeiros e agentes de fiscalização. Manter tais informações é importante tanto para a gestão de incidentes de segurança quanto para a gestão da continuidade dos negócios.

O DSIC publicou a Norma Complementar 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), que apresenta modelos de criação de ETIR para os órgãos da Administração Pública Federal (APF).

Exercício de fixação 6
Procedimentos da gestão de incidentes de segurança

O que deve ser contemplado nos procedimentos da gestão de incidentes de segurança?

Planos de contingências

Aspectos importantes:

- Recursos financeiros, humanos e de infraestrutura.

Fases:

- Resposta imediata a desastres.
- Processo de recuperação.

A seguir serão apresentados os aspectos relacionados à importância dos planos de contingência nas organizações e suas fases de planejamento.

Implementar (planejar, elaborar e implantar) um plano de contingências envolve recursos financeiros, acordos, cooperação dos funcionários e, muitas vezes, auxílio de consultorias técnicas externas e empresas especializadas em segurança ou seguros. Em adição, devem ser também considerados os custos com treinamentos, testes e manutenção do plano.

Um plano de contingências deve contemplar duas fases: resposta imediata a desastres (inclusive incidentes de segurança) e processo de recuperação. Na primeira fase, deve-se considerar as decisões gerenciais quanto às medidas a serem aplicadas e, na segunda fase, deve-se definir os procedimentos necessários ao restabelecimento das funções, sistemas e recursos. O plano de contingências pode incluir etapas distintas (e complementares) de recuperação, de modo que, ao longo do tempo, o funcionamento normal da organização seja restabelecido.

A seguir, serão apresentadas descrições de fases que compreendem o planejamento de contigências e os respectivos detalhes.

Fases do planejamento

- Atividades preliminares.
- Análise de impactos.
- Análise de alternativas de recuperação.
- Desenvolvimento do plano de contingências.

- Treinamento.
- Testes.
- Avaliação e atualização do plano.

Antes do planejamento, é importante responder às seguintes questões:

- Quais são os objetivos?
- Qual é o orçamento?
- Quais são os prazos?
- Quais são os recursos humanos disponíveis?
- Quais são os equipamentos e demais suprimentos necessários?
- Quais são as responsabilidades da equipe responsável pelo planejamento?

Com todas as respostas, pode-se iniciar o planejamento de contingências, seguindo as fases:

- Atividades preliminares, envolvendo a conscientização dos dirigentes da organização, a identificação dos recursos e informações críticas, análise de custos e definição de prazos;
- Análise de impacto, visando identificar os impactos causados por interrupção de serviços providos por cada sistema computacional da organização, considerando, para tanto, a importância de cada um deles para a continuidade dos negócios;
- Análise das alternativas de recuperação, que procura verificar a relação custo x benefício das várias opções para recuperação após desastres. É importante que, exatamente após essa fase, seja elaborado e entregue aos dirigentes da organização um documento relatando as análises e recomendações para a continuidade dos negócios;
- Desenvolvimento do plano de contingências após a análise do relatório apresentado ao final da fase anterior; tem por objetivo elaborar o conteúdo do plano;
- Treinamento, objetivando a conscientização das pessoas quanto a suas responsabilidades perante o plano;
- Teste do plano de contingências, visando identificar melhorias através de adaptações ou correções;
- Avaliação dos resultados e atualização do plano, na qual os resultados dos testes são avaliados e é iniciado o processo de modificação do plano conforme as melhorias propostas.

Atividades preliminares

- Iniciativas para a conscientização dos dirigentes.
- Levantamento preliminar de recursos, sistemas e funções críticas aos negócios.

As atividades preliminares do planejamento de contingências compreendem basicamente todas as iniciativas de conscientização dos dirigentes a respeito das necessidades e um estudo preliminar a respeito dos itens críticos para a organização.

Não é possível implantar um plano de contingências sem a real sensibilização dos dirigentes da organização, muito menos sem seu apoio total.

No estudo preliminar dos serviços críticos, são levantados recursos, sistemas e funções críticas aos negócios da organização, e também custos, prazos e recursos humanos necessários à realização da análise de impacto (a próxima fase do planejamento). Note aqui a importância de apresentar esse estudo aos dirigentes da organização, com o intuito de obter sua aprovação.

Exercício de fixação 7
Plano de contingências

Quais são as fases de um plano de contingência e o que deve ser contemplado em cada fase?

Quais são as atividades preliminares do planejamento de contingência?

Análise de impacto

Atividade importante para a tomada de decisões estratégicas. Subfases:

- Identificação e classificação dos recursos, sistemas e funções críticas.
- Definição do tempo para recuperação.
- Elaboração de relatório específico.

Nesta fase, são identificados e classificados, em função de sua importância para os negócios da organização, as funções, os sistemas e recursos, considerando, para tanto, as possíveis ameaças a que estão expostos. Essa análise é um elemento importante para que os dirigentes possam tomar decisões a respeito dos investimentos a serem aplicados em medidas de segurança, com vistas à continuidade de seus negócios.

No processo de análise de impactos, é importante realizar entrevistas com diferentes gerentes de equipe de setores específicos e críticos para os negócios da organização, equipes de suporte e usuários de sistemas.

A análise de impacto pode ser dividida em três subfases: identificação dos recursos, funções e sistemas críticos, definição do tempo para recuperação e elaboração de relatório.

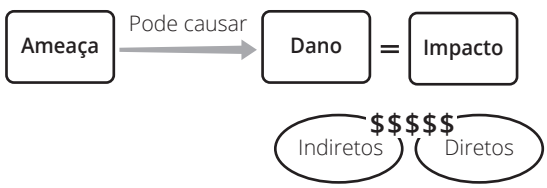


Figura 9.1
Sequência até o impacto.

Exercício de fixação 8
Análise de impacto

Especifique as subfases de uma análise de impacto:

Identificação dos recursos, funções e sistemas críticos

- Identificar e classificar segundo as prioridades para os negócios.
- Essencial à tomada de decisões quanto a contingências.

Nesta subfase, deve-se considerar tanto a identificação de recursos, funções e sistemas críticos, quanto sua classificação. Segue uma proposta para classificação que pode ser usada em organizações reais:

- Altamente importantes (essenciais);
- De importância média;
- De baixa importância.

Note que identificação e classificação geram dados essenciais à tomada de decisão a respeito do escopo do plano de contingência, garantindo um funcionamento da organização em um nível de serviço aceitável.

Definição do tempo para recuperação e elaboração de relatório

Determinar o intervalo de tempo aceitável para paradas. No relatório, destacar:

- Recursos, sistemas e funções identificadas e classificadas.
- Descrição das potenciais ameaças.
- Intervalo de tempo aceitável para recuperação.
- Levantamento de recursos necessários à recuperação após desastres.

Na subfase de definição do tempo para recuperação, determina-se o intervalo de tempo aceitável de indisponibilidade de cada função, recurso e sistema em função da criticidade e do impacto relativos. Como resultado, tem-se o intervalo de tempo aceitável para a recuperação do recurso, sistema ou função.

No relatório, deve-se destacar:

- Os recursos, sistemas e funções identificados e classificados em ordem de importância para a organização;
- Uma descrição das ameaças potenciais para cada recurso, sistema e função;
- O intervalo de tempo tolerável para a recuperação de cada recurso, sistema e função;
- O levantamento de recursos humanos, instalações, equipamentos e serviços requisitados para o restabelecimento e recuperação de cada recurso, sistema e função.

Ao final das três subfases, o relatório baseará os dirigentes da organização na tomada de decisão quanto à implantação do plano de contingências.

Análise de alternativas de recuperação

Considerar necessidades reais da organização. Existem várias alternativas:

- Prevenção e detecção de acidentes.
- Política adequada de backup.
- Armazenamento e recuperação de dados.
- Seguros.

Nesta fase, alternativas como prevenção e detecção de acidentes, controle de backups, estratégias confiáveis para armazenamento e recuperação de dados, seguros, espelhamento de sistemas e recursos, entre outras alternativas de recuperação no caso de desastres, são analisadas e selecionadas para serem implantadas em casos específicos de necessidade de contingência, considerando os resultados obtidos nas fases anteriores do planejamento.

Em termos de prevenção e detecção de acidentes, é recomendável considerar equipamentos de detecção e combate a incêndios; a manutenção preventiva de equipamentos; a proteção de documentos não magnéticos (impressos, por exemplo); a segurança adequada de recursos humanos etc.

A política de backup é um dos elementos mais importantes de um plano de contingências; afinal, um sistema que passou por problemas pode ser comparado com seu backup (se mantido atualizado e completo), possibilitando sua restauração. Portanto, cabe à política de backup determinar todos os procedimentos necessários à proteção das informações da organização de acordo com sua importância para os negócios. Vale lembrar que a infraestrutura e os procedimentos de backup devem ser testados regularmente, para que a recuperação, em caso de problemas de segurança, seja realmente assegurada.

Em termos de armazenamento de dados, deve-se considerar a segurança adequada aplicada à mídia e o local de armazenamento utilizado, inclusive considerando o armazenamento remoto de cópias. Para a recuperação de dados armazenados, é recomendado testar regularmente os procedimentos de restauração usados. Lembre-se de que, se a recuperação de dados for falha, de nada servirá manter backups.

Deve-se também considerar a possibilidade de contratar seguros para cobrir potenciais perdas causadas por incidentes de segurança.

Exercício de fixação 9
Análise de alternativas de recuperação

Por que a política de backup é importante em um plano de contingência?

Relatório de alternativas de recuperação

- Descrição das opções.
- Estimativas de custos.
- Vantagens e desvantagens.
- Recursos necessários.

Após a análise de alternativas, deve-se elaborar um relatório detalhado a respeito das opções para recuperação, estimativas de custos e vantagens e desvantagens de cada alternativa.

Cabe também destacar os recursos humanos, financeiros e de infraestrutura requeridos para a próxima fase. Tal relatório também apoiará os dirigentes da organização nas tomadas de decisão estratégicas quanto ao plano de contingência.

Desenvolvimento do plano de contingências

- Designar equipe responsável.
- Determinar como responder a desastres.
- Identificar aplicativos críticos.
- Manter inventário de arquivos, dados, Sistema Operacional e utilitários.
- Levantar necessidades especiais.

Durante o desenvolvimento do plano de contingências, deve-se atentar para as seguintes orientações, pelo menos:

- Designar uma equipe para implantar o plano de contingências, inclusive dividindo-a por área de atuação. Por exemplo, equipe gerencial, que tratará da coordenação das atividades relacionadas, e equipe de resposta imediata a incidentes, que acionará as medidas adequadas aos incidentes de segurança ocorridos;
- Determinar como responder a desastres em tempo hábil, contemplando a identificação e compreensão do problema; contenção de danos; identificação dos danos causados; restauração dos sistemas e eliminação das causas dos desastres;
- Identificar os aplicativos críticos, aos quais deverão ser aplicadas medidas emergenciais em situações de desastre;
- Manter um registro (ou inventário) de arquivos, dados, programas, Sistema Operacional e utilitários relacionados aos aplicativos críticos, assegurando que todos serão incluídos nos procedimentos de backup e recuperação;
- Levantar as necessidades de condições especiais requeridas por parte das redes de comunicação;
- Considerar cuidados como retirada de pessoal e garantia da segurança de documentos em papel e em meios magnéticos.

Treinamentos e testes

- Treinamentos devem ser regulares e compreender teoria, práticas e simulações.
- Testes podem ser feitos nas categorias:
  - Integral.
  - Parcial.
  - Simulado.

Deve-se considerar nesta fase iniciativas para a conscientização dos funcionários e terceiros quanto ao plano de contingências da organização. Sendo assim, os treinamentos devem ser regulares, envolvendo simulações, teoria e prática.

Uma das garantias que a organização pode considerar, em termos do plano de contingências, é o resultado dos testes aplicados a ele. Em termos práticos, os testes podem ser classificados nas seguintes categorias:

- Integral, envolvendo situações próximas à realidade da organização; por exemplo, contemplando a verificação de procedimentos de transferência de pessoas e processamento para locais de reserva;
- Parcial, restrita a partes do plano de contingências ou a certas atividades ou aplicativos;

- Simulado, considerando representações da situação de desastre; por exemplo, desocupação do prédio da organização em uma simulação de incêndio.

Durante os testes, deve-se cronometrar todos os eventos relacionados e registrar todos os problemas ocorridos, se possível indicando uma classificação de acordo com sua gravidade.

Exercício de fixação 10
Treinamentos e testes

Como podem ser classificados os testes?

Avaliação e atualização do plano

A avaliação e atualização do plano devem ser contínuas e refletir mudanças:

- Nos negócios.
- No ambiente.
- Em questões administrativas.

Em função de mudanças nos objetivos de negócio, mudanças administrativas e de ambiente computacional, por exemplo, deve-se também atualizar o plano de contingências, de modo que este reflita tais mudanças, minimizando impactos ocasionados por falhas de segurança.

Exemplos de recomendações para a prevenção de incidentes de segurança da informação:

- "Não é permitido, a menos que com a devida autorização, interferir, sobrecarregar ou desativar um serviço, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos."
- "É vetada aos usuários a execução de testes ou tentativas de comprometimento de controles internos. Esta prática é permitida apenas a pessoas com competência e função técnica na organização, durante atividades de monitoramento e análise de riscos, com a autorização legítima para tal."

Os exemplos apresentam algumas recomendações que podem fazer parte da política de segurança ou das diretrizes de segurança da informação, objetivando a ocorrência de incidentes de segurança. Todas as recomendações são consideradas genéricas e aplicáveis em organizações reais.

Boas práticas

- Documentar incidentes de segurança.
- Identificar recursos, sistemas e funções críticas.
- Analisar impactos.
- Avaliar alternativas e selecionar as adequadas.
- Elaborar o plano segundo as necessidades reais.
- Promover treinamentos periódicos.
- Efetuar testes regulares.
- Manter o plano atualizado.

Na procura por uma adequada gestão de incidentes e um plano de contingências efetivo para uma organização, algumas práticas são recomendadas:

- Documentar todos os incidentes de segurança e ações tomadas, para possibilitar uma investigação posterior das causas;
- Identificar recursos, funções e sistemas críticos e suas prioridades em função dos negócios;
- Analisar o impacto ocasionado por ameaças de segurança na organização;
- Avaliar alternativas de recuperação, procurando identificar as mais adequadas ao contexto;
- Elaborar o plano de contingências de acordo com os recursos disponíveis (financeiros, de recursos humanos e de infraestrutura);
- Treinar pessoas, conscientizando-as a respeito de suas responsabilidades junto ao plano de contingências;
- Efetuar testes regulares no plano de contingências e nos procedimentos de recuperação estabelecidos na organização.

Roteiro de Atividades 9

Atividade 9.1 – Entendendo os conceitos de Gestão de Continuidade de Negócios

1. Explique o que é a Gestão de Continuidade de Negócios.

2. Que considerações devem ser atendidas no tratamento da segurança da informação no contexto da continuidade de negócios?

Atividade 9.2 – Executando a continuidade de negócios

1. Qual a estrutura mínima de um Plano de Continuidade de Negócios (PCN)?

2. O que a gestão de incidentes de segurança deve contemplar?

3. Qual a importância da notificação de eventos adversos?

4. Quais devem ser os procedimentos da gestão de incidentes de segurança?

5. Descreva o que deve ser feito durante a análise de impacto no decorrer das fases do planejamento de contingências.

6. Explique o que é o "tempo de recuperação" e, através de um exemplo prático, indique como ele deve ser empregado.

Atividade 9.3 – Executando a continuidade de negócios e a gestão de incidentes na sua organização

1. Como integrante do comitê de segurança da informação, você foi indicado(a) para apresentar um plano de Continuidade de Negócios (PCN) para sua organização. Durante a apresentação do tema, considerando a atual estrutura e objetivos da sua instituição, que atividades devem ser listadas para desenvolver este plano?

2. Você assumiu a responsabilidade de estruturar uma equipe de Tratamento e Respostas a Incidentes para redes computacionais (ETIR) para sua organização. Como você vai estruturar esta equipe? Que profissionais da sua organização integrarão o ETIR? Quais serão os objetivos do ETIR?

10

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.

Em termos de legislação e direito digital no Brasil, serão apresentados os seguintes subtópicos:

- Importância da legislação, mostrando os itens relevantes, em termos de legislação, para a segurança da informação;
- Direito digital, apresentando a definição e questões relacionadas;
- Legislação e direito digital no Brasil, dando uma visão geral a respeito das leis vigentes atualmente, com respeito à tecnologia e segurança da informação;
- Direito digital e necessidades atuais, identificando as necessidades atuais quanto à ausência de legislação específica no que se refere ao direito digital no Brasil;
- Estudo de caso, objetivando apresentar uma atividade prática correspondente, com o intuito de oferecer aos participantes uma reflexão a respeito de possíveis medidas preventivas para o caso estudado.

Exercício de nivelamento 1
Conformidade

O que você entende por conformidade?

Como é feita a conformidade na sua instituição?

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).

É crescente a preocupação com a legislação e padrões relacionados à segurança da informação, dada a sua importância para a sociedade atual. Sendo assim, vários projetos legislativos, padrões e normas já foram definidos ou estão em evolução ou em desenvolvimento.

As leis, em particular, garantem a proteção dos direitos aplicáveis à segurança da informação e preveem sanções legais às situações de fraude. Com base em padrões e normas, as organizações podem estabelecer suas políticas de segurança e processo de auditoria adaptados ao seu ramo de negócio. Vale esclarecer que, na maioria dos casos, padrões têm âmbito internacional, enquanto normas e leis, âmbito nacional. Sendo assim, há variações quanto a padrões, normas e leis aplicadas em países distintos.

As organizações devem garantir proteção contra a violação de quaisquer leis criminais ou civis, estatutos, regulamentações, obrigações contratuais e requisitos de segurança da informação, objetivando a garantia de conformidade legal e da saúde institucional. Nesse contexto, recomendam-se os serviços de consultoria prestados por empresas ou profissionais especializados na área jurídica (direito digital) e da segurança da informação.

Na procura por conformidade legal, é salutar que a organização busque e se mantenha atualizada quanto à legislação vigente e normas e padrões de segurança aplicáveis. No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) estabelece normas a serem seguidas por produtos e serviços, inclusive aqueles relacionados à segurança da informação. Em nível internacional, destacam-se, na área, a International Organization for Standardization (ISO) e a International Electrotechnical Comission (IEC).

Entre as normas diretamente relacionadas à gestão da segurança da informação, destacam-se as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.

Direito digital

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

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

- Penal.
- Autoral.
- Contratual.

O direito digital compreende um conjunto de princípios fundamentais e instrumentos jurídicos que atendem aos requisitos da era digital e envolvem questões multidisciplinares relevantes, a saber: civil, trabalhista, constitucional, do consumidor, penal, autoral e 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?

Exemplo de recomendação para uso de recursos de TI, definida na política de segurança:

- "Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelo usuário no âmbito da infraestrutura de TI, ficando os transgressores sujeitos à lei penal, civil e administrativa, na medida da conduta, dolosa ou culposa, que praticarem."

A recomendação proposta no exemplo é aplicável às organizações, uma vez que seja devidamente documentada na política de segurança e que esta seja efetiva na organização, isto é, devidamente implementada, divulgada e exigida.

Exercício de fixação 1
Direito digital

O que é direito digital e como se aplica na sua organização?

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.

É fato que a tecnologia da informação avança a passos largos e a era digital se consolida; todavia, as leis que compreendem o direito digital no Brasil não conseguem acompanhar tal evolução. Pode-se notar tal evidência com base no histórico a seguir, que apresenta, por sua vez, algumas leis e códigos relacionados ao direito digital no Brasil.

É importante ressaltar, assim, que há responsabilidades civis e criminais para os que trabalham com tecnologia da informação e segurança da informação no Brasil. Portanto, organizações públicas e privadas, servidores públicos e funcionários devem conhecer suas responsabilidades e atribuições legais.

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

Exercício de fixação 2
Legislação aplicável à segurança da informação

Qual o objetivo do decreto 3.505, de 13 de junho de 2000?

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.

Tabela 10.1
Infrações digitais em ambiente corporativo.
Fonte: Patricia Peck Pinheiro Advogados.

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.

Em termos de necessidades atuais quanto à legislação e ao direito digital, há uma série de questões indefinidas, tais como as exemplificadas a seguir:

- Privacidade x monitoramento, por exemplo, quanto ao uso, por parte de funcionários, de endereço de e-mail corporativo para receber conteúdo privado;
- Segurança da informação x usuário, em particular, no sentido de estabelecer claramente os direitos e sanções legais aplicáveis em caso de problemas;
- Responsabilidades por atividades realizadas em equipamentos da empresa são relevantes, pois equipamentos são ativos e devem ser utilizados de modo a não ocasionar processos judiciais;
- Limites de responsabilidades em ambientes externos devem ser considerados ao lidarmos com soluções como acesso remoto à rede da organização ou soluções de home office;
- Quanto à necessidade da guarda da prova, documentos digitais, tais como e-mail, não possuem legislação específica que determine seu uso como prova.

Enquanto a legislação referente ao direito digital não for estabelecida por completo, regras claras para a conduta dos funcionários, dirigentes, terceirizados e demais envolvidos devem ser elaboradas pelas organizações. Tal conduta deve ser monitorada e controlada, e os usuários devidamente orientados a respeito de seus limites e responsabilidades quanto às ações realizadas na organização. É sempre importante lembrar que divulgar e orientar são os dois principais fatores para limitar riscos.

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.

Em 18 de novembro de 2011, foi sancionada a lei de acesso a informações públicas, Lei nº 12.527, de 18 de novembro de 2011, que foi regulamentada pelo Decreto Nº 7.724, de 16 de maio de 2012.

A Lei de Acesso a Informação (LAI) trata dos procedimentos a serem observados para o cumprimento do direito constitucional da garantia de acesso às informações. A LAI possui um princípio bastante simples: as informações referentes à atividade do Estado, em qualquer nível, são públicas, salvo exceções expressas na legislação. Dessa forma, ela regulamenta o direito à informação garantida pela Constituição Federal, no inciso XXXIII, do Capítulo I – dos Direitos e Deveres Individuais e Coletivos: "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".

Assim, a divulgação de informações ganha procedimentos para facilitar e otimizar o acesso. Existem duas vertentes principais para o acesso à informação: disponibilização para consulta, situação em que a informação é solicitada pelo interessado; e divulgação de informações de interesse coletivo ou geral através da publicação no site institucional.

O DSIC publicou em junho de 2013 a Norma Complementar nº 01/IN02/NSC/GSIPR e seus anexos (Anexo A e Anexo B) Disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas.

A Lei nº 12.527/11 prevê exceções ao acesso à informação nos seguintes casos de informações classificadas como sigilosas pelas autoridades competentes e as relacionadas às demais hipóteses legais de sigilo, como as informações pessoais, relativas à intimidade, vida privada, honra e imagem.

Nesse ponto, destaca-se a importância da área de TI da organização bem como dos procedimentos quanto à segurança da informação para que seja preservado o sigilo e a privacidade quando for o caso. Outro ponto importante é que para poder tratar adequadamente as informações, a organização necessita implementar uma política de classificação das informações (vide item 8.2 da ABNT NBR ISO/IEC 27002:2013 e Decreto Nº 7.845, de 14 de novembro de 2012). Ainda sobre classificação da informação, a ABNT tem a norma ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento 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.

Em termos da verificação da conformidade com requisitos legais, serão apresentados os seguintes subtópicos:

Legislação vigente, mostrando as questões importantes a considerar em termos de documentos legais da própria organização e da legislação vigente no Brasil.

Os tópicos Propriedade intelectual, Proteção de registros organizacionais, Proteção de dados e privacidade de informações pessoais, Prevenção do mau uso de recursos de processamento das informações e Controles de criptografia são apresentados com o objetivo de indicar algumas das preocupações com a segurança da informação e legislação vigentes nas organizações. Em particular, esses tópicos são devidamente documentados como recomendações nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.

Estude a seção 18 – Conformidade da norma ABNT NBR ISO/IEC 27002:2013.

Legislação vigente

Recomenda-se definir, documentar e manter:

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

É importante, nas organizações, considerar a legislação em termos de estatutos, regulamentos e contratos vigentes, além de considerar a legislação específica e vigente no país. Dessa forma, todos os requisitos envolvidos com tais itens devem ser definidos, documentados e mantidos na organização.

Concomitantemente, é relevante também definir e documentar todos os controles e responsabilidades exigidos para garantir os requisitos estatutários, regulamentares e contratuais.

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.

Recomenda-se, para qualquer material ou software proprietário protegido por lei de propriedade intelectual, implementar procedimentos adequados que garantam a conformidade da organização em relação a requisitos legais, regulamentares e contratuais.

Por exemplo, esses requisitos podem determinar restrições quanto à cópia de determinado material com direitos autorais ou, ainda, que somente seja utilizado material desenvolvido pela própria organização.

Aplicar cuidados contra a violação da propriedade intelectual é relevante, principalmente porque tal situação pode conduzir a ações legais civis e até criminais.

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.

Conforme vimos, as organizações devem se preocupar com a propriedade intelectual e, com isso, implementar procedimentos adequados que culminem com a proteção das organizações frente a questões legais, estatutárias e contratuais. Sendo assim, a norma ABNT NBR ISO/IEC 27002:2013 recomenda alguns cuidados relevantes, a saber:

- Divulgação de uma política de conformidade com os direitos de propriedade intelectual que, por sua vez, defina claramente o uso legal de qualquer material, software ou informação protegida contra a violação da propriedade intelectual;
- Em processos de aquisição de software, estes devem ser obtidos apenas a partir de fontes reconhecidas e de boa reputação;
- Manter todas as pessoas da organização, independentemente do cargo, conscientes a respeito das políticas de proteção da propriedade intelectual e das ações disciplinares a serem aplicadas nos casos de violação;
- Indicar cada ativo da organização que possua requisitos diretamente relacionados à proteção dos direitos de propriedade intelectual, mantendo, ainda, seu devido registro;
- Manter todas as evidências quanto a licenças, manuais e afins na organização;

Monitorar as licenças, visando garantir que o uso do número máximo de licenças adquiridas não seja excedido.

- Garantir que apenas software licenciado seja instalado.
- Implantar uma política para licenças.
- Estabelecer uma política para transferências de software.
- Utilizar ferramentas adequadas de auditoria.
- Cumprir termos e condições para software e informações obtidas de fontes públicas.
- Garantir a integridade de registros comerciais.
- Não copiar, em parte ou em todo, documentos com direitos autorais.
- Efetuar o controle quanto aos softwares, garantindo a instalação apenas daqueles licenciados e devidamente autorizados;
- Implantar uma política para a manutenção adequada das condições de licenças;

- Definir uma política para reger a transferência de softwares para outras organizações;
- Assegurar que as ferramentas de auditoria utilizadas são adequadas;
- Satisfazer a todos os termos e condições para materiais, softwares e informações obtidas a partir de redes públicas;
- Proteger registros comerciais, tais como filmes, áudios e outros, contra duplicações, conversões ou extrações não permitidas pela lei de direito autoral;
- Proteger partes ou a totalidade de livros, artigos, relatórios etc., contra cópias não autorizadas e violação da lei de direito autoral vigente.

Produtos de software proprietário são fornecidos sob um contrato de licenciamento que define os termos e condições da licença, como, por exemplo, limitando a cópia de um software apenas para a criação de uma cópia de segurança.

Direitos de propriedade intelectual são aplicados a softwares, documentos, projetos, marcas, patentes e licenças de códigos-fonte.

Exercício de fixação 3
Cuidados com a propriedade intelectual

Cite três cuidados com a proteção intelectual adotados pela sua instituição.

Proteção de registros organizacionais

- Recomenda-se proteger registros contra perdas, destruição ou falsificação.
- Recomenda-se classificar os registros da organização:
  - Registros de base de dados.
  - Registros de transações.
- Recomenda-se manusear e armazenar mídias de acordo com as recomendações do fornecedor.
- Nas organizações, recomenda-se proteger os registros categorizados como essenciais ao negócio contra perdas, destruição e falsificação, de modo a garantir conformidade com seus requisitos estatutários, regulamentares e contratuais.
- Alguns registros podem precisar ser retidos de forma segura para atender a requisitos estatutários, contratuais ou regulamentares ou, ainda, atender a requisitos do negócio. Por exemplo, aqueles registros que evidenciam a conformidade de uma organização perante os requisitos estatutários, regulamentares e contratuais que, assim, garantem a defesa da organização contra ações legais civis ou criminais.
- Em adição, os registros também podem ser categorizados com o objetivo de aplicar definições particulares, tais como o período de retenção e tipo de mídia de armazenamento. Por exemplo, registros de auditoria, registros da contabilidade e registros transacionais que possuem tempo de retenção de 6 meses, 1 ano e 3 meses, armazenados em meio magnético, papel e meio magnético, respectivamente.
- As chaves de criptografia usadas para garantir confidencialidade ou autenticidade de registros também devem ser armazenadas durante o tempo de retenção respectivo.
- Adicionalmente, considera-se que todas as mídias de armazenamento sejam protegidas contra deterioração se utilizadas de acordo com a prescrição do fornecedor.

Saiba mais

Mais informações a respeito de gerência de registros podem ser encontradas na norma ISO 15489-1.

O tempo de retenção aplicado a registros organizacionais (Tabela de Temporabilidade) é definido em leis e regulamentações nacionais, tais como a Resolução nº 14, de 24 de outubro de 2001 do Conselho Nacional de Arquivos (CONARQ), entre outras.

Cuidados para a proteção de registros organizacionais

- Estabelecer diretrizes para retenção, armazenamento, tratamento e disponibilidade de registros e informações.
- Definir um cronograma para retenção.
- Disponibilizar um inventário de fontes de informação cruciais para a organização.
- Implantar controles para a proteção dos registros e informações.

Consulte as normas e recomendações do Conselho Nacional de Arquivos (CONARQ): http://www.conarq.arquivonacional.gov.br

Para garantir a proteção dos registros de uma organização, a norma ABNT NBR ISO/IEC 27002:2013 recomenda os procedimentos a seguir:

- Estabelecimento de diretrizes para a retenção, armazenamento, tratamento e disponibilidade de registros e informações;
- Definir um cronograma para a retenção, de modo a indicar os registros essenciais e o respectivo período em que será aplicado;
- Manutenção de um inventário compreendendo as fontes de informações consideradas fundamentais para a organização;
- Implementação de controles adequados à proteção dos registros e informações.

Proteção de dados e privacidade de informações pessoais

- A proteção e a privacidade de dados e informações pessoais devem ser asseguradas na legislação, regulamentações e contratos.
- Na organização deve-se implantar, divulgar e efetuar a gestão de uma política de privacidade e proteção.

Nas organizações recomenda-se garantir a proteção de dados e a privacidade das informações pessoais, em conformidade com a legislação, regulamentos e contratos vigentes. Para tanto, as organizações podem criar uma equipe que definirá, implantará, divulgará e gerenciará uma política de proteção e privacidade, buscando, concomitantemente, a conformidade com a legislação, regulamentos e contratos vigentes. Vale ressaltar que todas as pessoas da organização devem ser orientadas para saber exatamente quais são suas responsabilidades perante a política.

Alguns países possuem leis que estabelecem o controle na coleta, processamento e transmissão de dados e informações pessoais, impondo responsabilidades legais aos diretamente envolvidos em tais etapas.

Prevenção do mau uso de recursos de processamento da informação

Recomenda-se proteger os recursos de processamento contra mau uso, por meio de monitoramento, ferramentas, ações disciplinares ou legais.

Mau uso significa:

- Uso não relacionado diretamente ao negócio da organização.
- Uso não autorizado.

Nas organizações, os recursos de processamento da informação apoiam o negócio; sendo assim, recomenda-se a proteção dos recursos de processamento da informação contra uso não autorizado ou com objetivos não relacionados ao negócio. Para tanto, pode-se empregar, por exemplo, o monitoramento adequado, ferramentas de apoio (SDI – Sistemas de Detecção de Intrusos), ações disciplinares ou legais. Em termos de monitoramento e uso de ferramentas, deve-se atentar para a legislação vigente. Muitas vezes, a organização deve divulgar a todos os usuários que os recursos de processamento da informação são monitorados.

Quanto aos usuários, uma boa prática é conscientizá-los quanto a seus direitos e deveres perante os recursos de processamento disponíveis na organização e na legislação vigente. Para exemplificar, pode-se requerer dos usuários a assinatura de uma declaração do conhecimento de suas responsabilidades no contexto. E, por conseguinte, tais declarações devem ser mantidas em segurança pela organização.

Controles de criptografia

Recomenda-se o uso de criptografia conforme os requisitos legais, regulamentares e contratuais vigentes. Algumas preocupações relacionadas:

- Restrições à importação e/ou exportação de hardware e software para criptografia.
- Restrições à importação e/ou exportação de hardware e software com criptografia embutida.
- Restrições quanto ao uso.
- Definição dos métodos de acesso à informação cifrada.

Nas organizações, o uso de criptografia deve ser efetuado em conformidade com a legislação, regulamentos, contratos e acordos. Sendo assim, a norma ABNT NBR ISO/IEC 27002:2013 recomenda as seguintes ações, em conformidade com a legislação nacional vigente:

Estude a seção 10 – Criptografia da norma ABNT NBR ISO/IEC 27002:2013.

- Restringir o uso de criptografia;
- Restringir importação e/ou exportação de hardware e software cujo objetivo é a execução de funções de criptografia;
- Restringir importação e/ou exportação de hardware e software projetados com funções de criptografia embutidas;
- Definir métodos de acesso à informação cifrada por hardware ou software a serem utilizados por autoridades de outros países.

Exemplo de recomendação para uso de recursos de TI, definida na política de segurança:

- "Os sistemas de TI deverão ser utilizados sem violação dos direitos de propriedade intelectual de qualquer pessoa ou empresa, como marcas e patentes, nome comercial, segredo empresarial, domínio na internet, desenho industrial ou qualquer outro material que não tenha autorização expressa do autor ou proprietário dos direitos relativos à obra artística, científica ou literária."

A recomendação proposta no exemplo é aplicável às organizações objetivando a proteção da propriedade intelectual, uma vez que seja devidamente documentada na política de segurança e que esta seja efetiva na organização, isto é, devidamente implementada, divulgada e exigida.

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.

Em termos da verificação da conformidade com políticas e normas de segurança da informação, serão apresentados os seguintes subtópicos: “Normas de segurança no Brasil”, mostrando as principais normas vigentes para o contexto. No tópico “Evolução das normas”, indica-se uma prospecção quanto à sua manutenção. Os tópicos “Conformidade com políticas e normas”, “Trabalhando as não-conformidades” e “Conformidade técnica” apresentam individualmente as preocupações e práticas a serem consideradas quanto às políticas e normas vigentes nas organizações.

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.

Em 2001, a ABNT disponibilizou a norma ABNT NBR ISO/IEC 17799, uma versão brasileira da BS ISO/IEC 17799, e, desde então, no Brasil, essa norma vem se destacando como uma das principais referências para a gestão da segurança da informação. Em seu conteúdo, a norma trata dos seguintes itens: política de segurança da informação, organização da segurança da informação, gestão de ativos, segurança em recursos humanos, segurança física e do ambiente, gestão de operações e comunicações, controle de acesso, aquisição, desenvolvimento e manutenção de sistemas de informação, gestão de incidentes de segurança da informação, gestão da continuidade de negócios e conformidades.

A seguir, é apresentado um histórico da evolução de padrões internacionais e normas vigentes no Brasil:

- Em 1995, é liberada a primeira versão da BS 7799-1 (BS 7799-1:1995 – Tecnologia da informação – Código de prática para gestão da segurança da informação).
- Em 1998, é liberada a primeira versão da BS 7799-2 (BS 7799-2:1998 – Sistema de gestão da segurança da informação – Especificações e guia para uso).
- Em 1999, é liberada a revisão da BS 7799-1:1995.
- Em 2000, é liberada a primeira versão do padrão internacional BS ISO/IEC 17799 (BS ISO/IEC 17799:2000 – Tecnologia da informação – Código de prática para gestão da segurança da informação).
- Em 2001, a ABNT homologou a NBR 17799, versão brasileira da BS ISO/IEC 17799 (ABNT NBR ISO/IEC 17799:2001 – Tecnologia da informação – Código de prática para gestão da segurança da informação).
- Em 2002, é liberada a revisão da BS 7799-2:1998.

- Em agosto de 2005, é liberada a segunda versão da ABNT NBR ISO/IEC 177799 (ABNT NBR ISO/IEC 17799:2005 – Tecnologia da informação – Código de prática para gestão da segurança da informação).

Evolução das normas

- Família de normas para o SGSI, sob a denominação ISO/IEC JTC 1/SC 27.
- Liberadas usando a série de números 27000, em sequência.
- Em 2007, a nova versão da ISO/IEC 17799 foi incorporada à ISO/IEC 27002.

A ISO desenvolve uma família de normas para o Sistema de Gestão da Segurança da Informação (SGSI), cujo conteúdo engloba os requisitos de tais sistemas, gestão de riscos, métricas e medidas de segurança da informação e diretrizes para implementação. A denominação a ser usada é a ISO/IEC JTC 1/SC 27, a serem liberadas em sequência, usando a série de números 27000.

Em 2006, a ABNT homologou a NBR 27001, versão brasileira da ISO/IEC 27001, que possui a seguinte nomenclatura: ABNT NBR ISO/IEC 27001:2001 – Tecnologia da informação – Sistema de gestão da segurança da informação. A versão atual foi publicada pela ABNT em novembro de 2013 com a seguinte nomenclatura: ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – Sistema de gestão da segurança da informação – Requisitos.

Atualmente para a área de segurança da informação estão publicadas, pela ABNT ou pela ISO, as seguintes normas:

- ABNT NBR ISO/IEC 27003:2011 – Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação.
- ABNT NBR ISO/IEC 27004:2010 – Tecnologia da informação – Técnicas de segurança – Gestão da segurança da informação – Medição.
- ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
- ABNT NBR ISO/IEC 27007:2012 – Diretrizes para auditoria de sistemas de gestão da segurança da informação.
- ABNT NBR ISO/IEC 27011:2009 – Tecnologia da informação – Técnicas de segurança – Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002.
- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da Informação – Técnicas de Segurança – Governança de segurança da informação.
- ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário.
- ABNT NBR 15999-1:2007 – Versão Corrigida:2008 – Gestão de continuidade de negócios – Parte 1: Código de prática.
- ABNT NBR 16167:2013 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação.
- ISO/IEC 27000:2014 – Information technology – Security techniques – Information security management systems - Overview and vocabulary.
- ISO/IEC 27006:2011 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.

- ISO/IEC TR 27008:2011 – Information technology – Security techniques – Guidelines for auditors on information security controls.
- ISO/IEC 27010:2012 – Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications.
- ISO/IEC TR 27019:2013 – Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.
- ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity.
- ISO/IEC 27033-2:2012 – Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security.
- ISO/IEC 27034-1:2011 – Information technology – Security techniques – Application security – Part 1: Overview and concepts.
- ISO/IEC 27035:2011 – Information technology – Security techniques – Information security incident management.
- ISO/IEC 18028-4:2005 – Information technology – Security techniques – IT network security –Part 4: Securing remote access.
- ISO/IEC 18028-5:2006 – Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks.
- ISO/IEC 18033-4:2011 – Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers.
- ISO/IEC 29192-1:2012 – Information technology – Security techniques – Lightweight cryptography – Part 1: General.
- ISO/IEC 29192-2:2012 – Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers.
- ISO/IEC 11770-5:2011 – Information technology – Security techniques – Key management – Part 5: Group key management.
- ISO/IEC 24760-1:2011 – Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts.
- ISO/IEC 29128:2011 – Information technology – Security techniques – Verification of cryptographic protocols.
- ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy framework.
- ISO 22320:2011 – Societal security – Emergency management – Requirements for incident response.

Segurança da informação na Administração Pública Federal

No âmbito da Administração Pública Federal (APF), através do Decreto nº 7.411, de 29 de dezembro de 2010, a responsabilidade pelo assessoramento e coordenação das atividades de segurança da informação e da proteção das infraestruturas críticas é competência exclusiva do Gabinete de Segurança Institucional da Presidência da República (GSIPR).

Através da Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências, foi publicado como a APF deve tratar a gestão da segurança da informação. Nesta IN destacam-se:

Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

- ...
- IV – nomear Gestor de Segurança da Informação e Comunicações.
- V – instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais.
- VI – instituir Comitê de Segurança da Informação e Comunicações.
- VII – aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações.

O GSI exerce suas atividades de segurança da informação através do seu Departamento de Segurança da Informação e Comunicação (DSIC), que possui, entre outras, as seguintes missões:

Departamento de Segurança da Informação e Comunicação (DSIC):

- Planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal.
- Definir requisitos metodológicos para implementação da segurança cibernética e da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal.
- Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal.
- Planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal.
- Definir requisitos metodológicos para implementação da segurança cibernética e da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal.
- Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal.

O DSIC é responsável pela publicação das normas complementares para a APF. Atualmente existem as seguintes:

- Norma Complementar nº 01/IN01/DSIC/GSIPR, de 15 Out. 2008 – Atividade de Normatização;
- Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 Out. 2008 – Metodologia de Gestão de Segurança da Informação e Comunicações;
- Norma Complementar nº 03/IN01/DSIC/GSIPR, de 03 Jul. 2009 – Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;
- Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, (Revisão 01), de 15 Fev 2013 – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos e entidades da Administração Pública Federal;
- Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 Ago. 2009 – Disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal;

- Norma Complementar nº 06/IN01/DSIC/GSIPR, de 23 Nov. 2009 – Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
- Norma Complementar nº 07/IN01/DSIC/GSIPR, de 07 Mai. 2010 – Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
- Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 Ago. 2010 – Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;
- Norma Complementar nº 09/IN01/DSIC/GSIPR, (Revisão 01), de 15 Fev 2013 – Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta. E a Portaria Nº 10, de 20 de março de 2013, que da nova redação ao item 5.5 e inclui os subitens 5.5.1 e 5.5.2 na Norma Complementar nº 09/IN01/DSIC/GSIPR (Revisão 1);
- Norma Complementar nº 10/IN01/DSIC/GSIPR, de 10 Fev. 2012 – Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
- Norma Complementar nº 11/IN01/DSIC/GSIPR, de 10 Fev. 2012 – Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;
- Norma Complementar nº 12/IN01/DSIC/GSIPR, de 10 Fev. 2012 – Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
- Norma Complementar nº 13/IN01/DSIC/GSIPR, de 10 Fev. 2012 – Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);
- Norma Complementar nº 14/IN01/DSIC/GSIPR, de 10 Fev. 2012 – Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
- Norma Complementar nº 15/IN01/DSIC/GSIPR, de 21 Jun. 2012 – Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
- Norma Complementar nº 16/IN01/DSIC/GSIPR – Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta;
- Norma Complementar nº 17/IN01/DSIC/GSIPR, de 09 Abr 2013 – Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF);
- Norma Complementar nº 18/IN01/DSIC/GSIPR, de 09 Abr 2013 – Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

Conformidade com políticas e normas

Lembre-se de que a segurança da informação deve ser analisada periodicamente, e a análise deve se basear nas políticas e normas em uso. Portanto, as organizações devem assegurar conformidade com as políticas e normas de segurança da informação.

Como se sabe, a política de segurança de uma organização estabelece regras a serem seguidas para garantir a segurança de seus ativos. Em adição, existem normas que apoiam as organizações nesta tarefa. Sendo assim, as organizações devem garantir que seus sistemas estejam de acordo com as políticas e normas aplicadas para assegurar a segurança da informação, uma vez que a segurança é um aspecto a ser analisado periodicamente e tendo como base as políticas empregadas. Em particular, a norma ABNT NBR ISO/IEC 27002:2005 recomenda que os sistemas de informação devem ser auditados segundo as normas de segurança da informação implantadas.

Saiba mais

Além dessas normas complementares, toda a legislação pertinente à segurança da informação na APF e no Brasil pode ser encontrada na íntegra no site do DSIC: http://dsic.planalto.gov.br/legislacaodsic/

Trabalhando as não-conformidades

Ao encontrar uma não-conformidade durante o processo de verificação de conformidade com políticas e normas de segurança, a norma ABNT NBR ISO/IEC 27002:2013 recomenda:

- Determinar as causas da não-conformidade.
- Avaliar a necessidade de ações para a não repetição da não-conformidade.
- Aplicar ação corretiva.
- Analisar a ação corretiva aplicada.

É importante, ainda, manter registros de todos os resultados obtidos nas recomendações acima.

Conformidade técnica

Sistemas de informação devem ser periodicamente verificados em sua conformidade técnica, que pode ser realizada de duas maneiras:

- Manualmente, auxiliada por ferramentas de apoio.
- Por engenheiro de sistemas experiente, auxiliado por ferramentas automatizadas.

Testes devem ser planejados, documentados e repetidos.

Nas organizações, é importante efetuar a verificação periódica da conformidade de seus sistemas de informação com as normas de segurança da informação implementadas. Para tanto, podem ser utilizados, por exemplo, testes de invasão previamente planejados, durante os quais documentam-se os resultados com a possibilidade de repeti-los quantas vezes for necessário.

A verificação da conformidade técnica pode ser feita:

- Manualmente, auxiliada por ferramentas de apoio;
- Por um especialista, auxiliado por ferramentas automatizadas para a geração de relatório técnico.

Exemplos de recomendações para a conformidade:

- Código de ética e conduta profissional.
- Uso de um modelo adequado de identidade digital.
- Avisar adequadamente a respeito de monitoramento no ambiente eletrônico.

- Atualizar contratos que envolvam cláusulas sobre segurança da informação.
- Definir e publicar políticas objetivas e claras.
- A política de segurança da informação deve ser atualizada, clara e objetiva.

A seguir alguns exemplos de recomendações gerais relacionadas aos cuidados quanto à conformidade com políticas e normas de segurança da informação:

- Definição de um código de ética e conduta profissional, tratando os aspectos da tecnologia e da informação;
- Definição de um modelo técnico-legal de identidade digital, que pode, por exemplo, especificar o uso de crachás e certificados digitais, entre outros;
- Cuidados adequados com avisos de monitoramento no ambiente, em termos de rede, serviços de internet, entre outros;
- Manutenção dos contratos com cláusulas sobre segurança da informação, observando controles, auditorias, direitos de propriedade intelectual etc.;
- Definição formal e publicação de políticas, tanto interna quanto externamente à organização.

Exercício de fixação 4
Conformidade técnica

Explique o que vem a ser conformidade técnica.

Auditoria de sistemas de informação

Recomenda-se proteger:

- Os sistemas e as ferramentas usadas na auditoria de sistemas de informação.
- A integridade das ferramentas de auditoria.
- Contra o uso não autorizado das ferramentas de auditoria.

Em termos de considerações quanto à auditoria, serão apresentados os seguintes subtópicos:

- Auditoria, mostrando as principais necessidades de proteção quanto aos instrumentos utilizados pelo processo nas organizações.
- Cuidados durante a auditoria, alertando para algumas das preocupações relevantes a um processo adequado de auditoria na organização, com o objetivo de garantir a sua conformidade com a legislação, políticas e normas vigentes.

Durante a auditoria de sistemas de informação, recomenda-se proteger os sistemas e ferramentas empregados, garantindo sua integridade e controle contra acessos não autorizados. Sendo assim, as atividades de auditoria devem ser realizadas segundo um planejamento adequado, de comum acordo com os dirigentes da organização, de modo a não influenciar seu negócio.

O acesso às ferramentas de auditoria deve ser controlado, e elas devem ser armazenadas em locais separados ou isolados.

Cuidados na auditoria

- Auditoria acordada com a organização.
- Escopo da verificação acordado e controlado.
- Verificação limitada ao acesso apenas para leitura.
- Acessos além da leitura feitos em cópias isoladas, com sua remoção (ou armazenamento com segurança) ao final.
- Recursos usados identificados e disponíveis.
- Acessos monitorados e registrados.
- Tudo deve ser documentado.

A auditoria deve ser realizada após o acordo formal com os dirigentes da organização. Todas as verificações de conformidade devem ser executadas segundo o acordo formal estabelecido e devidamente controladas. Em particular, recomenda-se que a verificação seja limitada ao acesso apenas à leitura e, quando for necessário o acesso além desta, devem ser geradas cópias para uso. Essas cópias devem ser isoladas e armazenadas de modo seguro ou removidas ao final da auditoria. Os recursos devem ser todos identificados unicamente na organização para, assim, serem disponibilizados à auditoria. Todos os acessos devem ser controlados, ou seja, monitorados e registrados. Por fim, todo o processo deve ser documentado.

Outros padrões relevantes

Control Objectives for Information Technologies (CobiT 4.1):

- Framework de governança em TI, apresentando boas práticas para o controle de requisitos, mapas de auditoria, questões técnicas e riscos de negócio.

Information Technology Infrastructure Library (ITIL):

- Compreende uma biblioteca de boas práticas para a gestão de TI de domínio público, focando o cliente e a qualidade dos serviços de TI, estabelecendo um conjunto de processos e procedimentos gerenciais.

Control Objectives for Information Technologies (CobiT 4.1) é um framework de governança em TI, que apresenta boas práticas para o controle de requisitos, mapas de auditoria, questões técnicas e riscos de negócio; consiste em quatro domínios: Plan and organize, Acquire and implement, Deliver and support e Monitor and evaluate.

Recomenda-se o uso de CobiT como meio para otimizar os investimentos em TI, maximizando o ROI (do inglês Return Of Investments) e fornecendo métricas para avaliação de resultados.

Há preocupação com segurança nos domínios CobiT, por exemplo, no processo Define the information architecture process; no domínio Plan and organize existem o esquema de classificação de dados e os níveis de segurança.

O CobiT 5 foi lançado em abril de 2012, consolidando e integrando o CobiT 4.1, Val IT 2.0 e frameworks de risco de TI. Alinha-se com estruturas e padrões, como o Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO), Body Project Management of Knowledge (PMBOK), PRINCE2 e The Open Group Architecture Framework (TOGAF). Esta versão incorpora as últimas novidades em governança corporativa e técnicas de gerenciamento.

Information Technology Infrastructure Library (ITIL) compreende uma biblioteca de boas práticas (políticas, processos, procedimentos e instruções de trabalho) para a gestão de TI

O COBIT5 trata da governança corporativa e possui entre seus produtos dois guias profissionais direcionados a segurança da informação:
- COBIT5 for Information Security e
- COBIT 5 for Risk
Demonstra a importância que os temas segurança da informação e gestão de riscos têm para a governança corporativa.

de domínio público, focando no cliente e na qualidade dos serviços de TI e estabelecendo um conjunto de processos e procedimentos gerenciais organizados em disciplinas. Tornou-se o padrão BS-15000, anexo à ISO 9000:2000.

Navegue no CobiT Publications and Downloads: www.isaca.org/cobit

Em particular, a Operations Level Agreement (OLA) e a Service Level Agreement (SLA) são parte do processo ITIL de segurança da informação, englobando informações como métodos de acesso permitidos, acordos a respeito de auditoria e logging, medidas de segurança física, treinamento de usuários, procedimentos de autorização dos usuários e acordos para reportar e investigar incidentes de segurança.

Outras legislações pertinentes

- Lei nº 9.983, de 14 de julho de 2000 – Altera o Decreto Lei nº 2848/40 – Código Penal – tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
- Decreto 1.171, de 24 de junho de 1994 – Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;
- Código Processo Penal – Lei 3.689, de 03 de outubro de 41, atualizado até as alterações introduzidas pelas Leis nº 11.900, de 08.01.09;Código de Processo Civil – Lei 5.869, de 11 de janeiro de 1973;Art. 6º da Lei nº 10.683, de 28 de maio de 2003;
- Art. 8º do Anexo I do Decreto nº 5.772, de 8 de maio de 2006;Lei nº 7.232 de 29 de Outubro de 1984 – Política Nacional de Informática, e dá outras providências;
- Lei nº 8.027 de 12 de abril de 1990 – Normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;
- Lei nº 8.112 de 11 de dezembro de 1990 – Regime jurídico dos servidores públicos civil da União, das autarquias e das fundações públicas federais;
- Lei nº 8.429 de 2 de junho de 1992 – sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências;
- Decreto nº 6.029 de 1 de fevereiro de 2007 – Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;
- Lei nº 8.159 de 8 de janeiro de 1991 – Política nacional de arquivos públicos e privados e dá outras providências;
- Decreto nº 1.048 de 21 de janeiro de 1994 – Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências;
- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- 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;
- Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
- Acórdão 1603/2008 do Plenário do Tribunal de Contas da União – TCU;
- Guia de elaboração do PDTI do SISP (http://www.sisp.gov.br/guiapdti/wiki/Apresentacao);
- Contratações de Soluções de Tecnologia da Informação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP.

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?

Bibliografia

- BEZERRA, E. K.; GESTÃO DE RISCOS DE TI. Escola Superior de Redes/RNP, 2011.
- CAUBIT, R.; BASTOS, A. ISO 27001 e 27002 Uma visão prática. Editora Zouk, 2009.
- DIAS, C. Segurança e auditoria da tecnologia da informação. Axcel Books, 2000.
- FONTES, E. Políticas e Normas para a Segurança da Informação. Brasport, 2012.
- KUROSE, J. F.; ROSS, K. W. Redes de computadores e a Internet. Pearson Education do Brasil, 2003.
- LYRA, M. R.; SEGURANÇA E AUDITORIA EM SISTEMA DE INFORMAÇÃO. CIÊNCIA MODERNA, 2008.
- PECK, Patrícia. Direito digital: gestão do risco eletrônico. Aspectos legais e éticos do uso da tecnologia. Palestra no evento "Marketing político e Internet", 2006.
- TITTEL, E. Rede de computadores. Coleção Schaum. Bookman, 2003.
- SEMOLA, Marcos. GESTÃO DA SEGURANÇA DA INFORMAÇÃO – UMA VISÃO EXECUTIVA. Campus, 2003
- STALLINGS, W. Network security essentials. Prentice Hall, 2000.
- ABNT ISO GUIA 73:2009. Gestão de riscos – Vocabulário.
- Norma ABNT NBR ISO/IEC 27001:2013. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.
- Norma ABNT NBR ISO/IEC 27002:2013. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
- Norma ABNT NBR ISO/IEC 27003:2011. Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação.
- Norma ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
- Norma ABNT NBR ISO 55000:2014 Gestão de ativos — Visão geral, princípios e terminologia.
- Norma ABNT NBR ISO 55001:2014 Gestão de ativos — Sistemas de gestão — Requisitos.

- Padrão ISO/IEC TR 13335-3. Guidelines for the management of IT security: techniques for the management of IT security, 1998.
- Norma ISO/IEC 18028. Information technology – Security techniques – IT network security, 2005.
- Norma NBR 15999-1 e 2.
- Site DSIC: http://dsic.planalto.gov.br (acessado em dez. 2013).
- Site GSI: www.gsi.gov.br (acessado em dez. 2013).

Flávia Estélia Silva Coelho possui Bacharelado em Ciência da Computação e Mestrado em Informática pela Universidade Federal de Campina Grande. Desde 2001, atua em ensino de Graduação e Pós-Graduação Lato Sensu, em projetos de pesquisa e desenvolvimento nas áreas de computação distribuída e segurança da informação. É professora efetiva da Universidade Federal Rural do Semi-Árido (UFERSA), desde 2009, e Java Champion (Oracle), desde 2006.

Luis Geraldo Segadas de Araújo possui especialização em Gestão de Segurança de Informação, Redes de Computadores e Infraestrutura Computacional. Trabalhou para diversas empresas, entre elas a Fundação Petros, tendo atuado também como consultor, com destaque no BNDES e na TBG. Possui experiência em ensino, tendo sido professor na Universidade Estácio de Sá e no Infnet, além de instrutor na RNP/ESR. Possui amplo conhecimento em normas, em especial nas ISO/IEC 27001 e 27002. É Bacharel em Sistemas de Informação pela PUC-RJ, Pós-graduado em Redes de Computadores pela UFRJ e mestre em Administração de Empresas, também na PUC-RJ. Possui as certificações CISSP, CISA e CISM, sendo capacitado em planejamento, elaboração de política de segurança, normas, análise de riscos, diagnóstico e auditoria. Atualmente mora no Canadá.

Edson Kowask Bezerra é profissional da área de segurança da informação e governança há mais de quinze anos, atuando como auditor líder, pesquisador, gerente de projeto e gerente técnico, em inúmeros projetos de gestão de riscos, gestão de segurança da informação, continuidade de negócios, PCI, auditoria e recuperação de desastres em empresas de grande porte do setor de telecomunicações, financeiro, energia, indústria e governo. Com vasta experiência nos temas de segurança e governança, tem atuado também como palestrante nos principais eventos do Brasil e ainda como instrutor de treinamentos focados em segurança e governança. É professor e coordenador de cursos de pós-graduação na área de segurança da informação, gestão integrada, de inovação e tecnologias web. Hoje atua como Coordenador Acadêmico de Segurança e Governança de TI da Escola Superior de Redes.

esr.rnp.br

LIVRO DE APOIO AO CURSO

O curso desenvolve competências para a implementação da gestão da segurança da informação, ccom base nas normas de segurança ABNT NBR ISO/IEC 27001:2013 e IEC 27002:2013. Através delas serão estudados os conceitos de política de segurança e gestão de riscos, como também as boas práticas para a segurança de recursos humanos e computacionais, segurança física e noções de direito digital. O curso garante ao aluno todo o conhecimento necessário para iniciar um processo de implementação da gestão da segurança da informação na sua instituição.

Este livro inclui os roteiros das atividades práticas e o conteúdo dos slides apresentados em sala de aula, apoiando profissionais na disseminação deste conhecimento em suas organizações ou localidades de origem.

ISBN 978-85-63630-12-4