Escola Superior de Redes RNP

Políticas de **Segurança da Informação**

Edison Luiz Gonçalves Fontes

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**

Políticas de **Segurança da Informação**

Edison Luiz Gonçalves Fontes

Políticas de **Segurança da Informação**

Edison Luiz Gonçalves Fontes

Rio de Janeiro
Escola Superior de Redes
2015

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
Lincoln da Mata

Revisão técnica
Carla Freitas
Edson Kowask Bezerra

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

Capa, projeto visual e diagramação
Tecnodesign

Versão
1.0.0

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)

B277p Gonçalves, Edison Luiz
Políticas de segurança da informação / Edison Luiz Gonçalves Fontes. – Rio de Janeiro: RNP/ESR, 2015.
126 p. : il. ; 27,5 cm.

Bibliografia: p.113.
ISBN 978-85-63630-37-7

1. Planejamento estratégico. 2. Tecnologia da informação – gestão. 3. Sistemas de informação. I. Brodbeck, Angela. II. Titulo.

CDD 658.4/038

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 curso apresenta o processo para desenvolver políticas de segurança da informação necessárias para que a organização planeje, construa, implante e mantenha a política de segurança da informação. Este conjunto de documentos formados por diretrizes, normas e procedimentos, formam a Política de Segurança da Informação da Organização. Através deste curso o aluno avaliará políticas em uso por organizações, escreverá sua própria política de segurança da informação considerando o seu ambiente profissional e levará para a sua organização uma primeira versão de alguns regulamentos de segurança da informação. O curso baseia-se nas boas práticas para o desenvolvimento das políticas e ainda nas recomendações da NC 03/IN01/DSIC/GSIPR - DIRETRIZES PARA ELABORAÇÃO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL.

A quem se destina

O curso destina-se aos gestores e profissionais de TIC que necessitam desenvolver e implementar políticas de segurança da informação. Também poderão participar quaisquer outros profissionais que desejem obter e desenvolver competências sobre políticas de segurança.

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 aúdio 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: TORRES, Pedro et al. *Administração de Sistemas Linux: Redes e Segurança*. Rio de Janeiro: Escola Superior de Redes, RNP, 2013.

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

Edison Fontes é Mestre em Tecnologia pelo Centro Paula Souza do Governo do Estado de São Paulo; Bacharel em Informática pela UFPE, Certificado CISM, CISA e CRISC pela ISACA/USA, Professor em Cursos de Pós Graduação e Palestrante Corporativo. É autor de cinco livros sobre Segurança da Informação pelas Editoras Sicurezza, Saraiva e Brasport. Dedica-se ao assunto Segurança da Informação desde 1989. Desenvolveu Politicas de Segurança para várias Organizações, com destaque para o NOSI-Núcleo Operacional da Sociedade da Informação do Governo de Cabo Verde que foram transformadas em Lei. Exerceu a função de Security Officer em instituições financeiras (Banco BANORTE e RBS-Royal Bank of Scotland-Brasil) e em empresa de serviços de alta disponibilidade (GTECH Brasil). Atualmente desenvolve atividades como Consultor em Segurança da Informação.

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.

Carla Freitas é formada em Ciência da Computação pela Universidade Federal da Bahia e possui pós-graduação em Redes e Segurança da Informação pela Faculdades Ruy Barbosa. Possui as certificações Auditor e Implementador Lider ISO/IEC 27001 e QSP ISO 31000 - Gestão de Riscos e auditoria baseada em riscos.Com 13 anos de experiência em segurança, atua como coordenadora no Centro de Atendimentos a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa (CAIS/RNP), onde é responsável pelo desenvolvimento de políticas de segurança, realização de análises de riscos e auditorias de conformidade.

1

Fundamentos de Política e Segurança da Informação

objetivos

Conhecer os conceitos, fundamentos e requisitos para o desenvolvimento ou implantação e o seu relacionamento com as normas e as estruturas conceituais que influenciam a Segurança da Informação.

conceitos

A informação; Processo Organizacional de Segurança da Informação; Dimensões de Segurança da Informação; Dimensão Política de Segurança da Informação; Política de Segurança da Informação como elemento das estruturas teóricas (norma ISO/IEC 27002, norma ISO/IEC 27001, norma ISO/IEC 27005, governança de Segurança da Informação, COBIT e ITIL).

Exercício de nivelamento
Segurança da Informação

Considerando a sua experiência profissional, qual a maior dificuldade para o sucesso da segurança da informação nas organizações?

A informação

Importante para a humanidade desde o seu surgimento, também é necessária para o desenvolvimento das organizações.

- Que precisam adotar um Processo Organizacional de Segurança da Informação.
- E criar uma política de segurança da informação.

A informação é o elemento básico para a humanidade desde o início da sua existência. Nosso organismo troca constantemente informações com elementos internos e externos. A temperatura do nosso corpo sobe e desce dependendo das condições internas e externas, e tudo isso acontece por causa da troca de informações entre as partes do nosso corpo. O não entendimento correto da informação faz com que o cérebro tome decisões erradas e consequentemente emita comandos inadequados. Tudo por causa de uma falha na

comunicação da informação. A informação é vital para o ser humano. No processo de crescimento, a criança recebe das pessoas que a cercam informações que as ensinarão a andar adequadamente, a comer e a se comportar em sociedade. As informações pessoais são recursos de valor e precisam ser protegidas contra o uso criminoso.

Para as organizações, a informação também é um elemento crítico. Sem informação, nenhuma organização sobrevive, nenhuma organização se mantém no seu mercado de atuação. A informação possibilita que a direção elabore seu planejamento estratégico-tático e que as atividades operacionais sejam realizadas e controladas.

O Tribunal de Contas da União reconhece essa importância da informação quando, no seu *Manual de Boas Práticas em Segurança da Informação*, declara (Brasil, TCU, 2012, página 10):

"Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações."

O manual continua esclarecendo sobre a importância da informação, sobretudo com os recursos de tecnologia (Brasil, TCU, 2012, página 7):

"Com a chegada dos computadores pessoais e das redes de computadores, que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das instituições modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável."

De uma maneira simplificada, todas as organizações possuem pelo menos dois elementos básicos para realizar adequadamente e com sucesso o seu negócio:

- O produto que será fabricado ou o serviço a ser prestado;
- A informação necessária para que esse produto-serviço seja produzido-prestado.

Em alguns casos, o produto-serviço a ser fabricado-prestado é também uma informação. Nesse caso, essa organização (ou parte da organização) tem a informação como meio e como produto-serviço final. Essa é a informação que a organização produz e gerencia.

Há outra informação que afeta fortemente a organização: é a informação que o mercado possui ou a informação que o mercado interpreta sobre a organização. Nesse caso, a organização tem poder menor sobre essa informação e sobre como o mercado tratará essa informação. Uma informação (verdadeira ou falsa) sobre a situação de uma organização pode levar o mercado no qual a organização atua a deixar de operar com ela. E mesmo que a organização não esteja em uma situação delicada, ficará em situação bem difícil. Essa questão está ligada à gestão da imagem da organização, à gestão de crises – enfim, à gestão do ambiente com o qual a organização se relaciona.

Mas nessas situações de trabalho interno e de relacionamento com o mercado, a informação é um elemento crítico, fundamental, essencial e muito valioso. A informação tem valor. Um valor que engloba, mas extrapola a questão monetária. A informação tem valor

institucional. Uma organização depende do tratamento que dá à informação para o seu sucesso ou insucesso. Uma organização que deseja atingir seus objetivos organizacionais, que deseja permanecer (e crescer) no seu ambiente de atuação precisa tratar a informação de maneira profissional. Ela precisa proteger a sua informação.

Para proteger a sua informação de maneira profissional, a organização precisa ter um Processo Organizacional de Segurança da Informação, que tem por objetivo permitir e possibilitar que a organização funcione adequadamente, ao depender da informação e dos recursos de informação.

Para que o Processo Organizacional de Segurança da Informação seja desenvolvido, implantado e mantido ao longo do tempo na organização, é necessária a existência, entre outros elementos, de regras para a utilização da informação. É necessária a existência de uma política de segurança da informação.

O processo organizacional de segurança da informação

A proteção da informação é uma responsabilidade da organização e deve se materializar pela atuação dos gestores dessa organização. A segurança da informação existe para proteger os recursos de informação, que possibilitam a organização atingir os seus objetivos institucionais e de negócio. Dessa maneira, definimos que a Segurança da Informação é um processo organizacional que tem por objetivo permitir e possibilitar que a organização alcance seus objetivos, no que depender da informação e dos recursos de informação.

O Processo Organizacional de Segurança da Informação precisa garantir para a informação a sua:

Confidencialidade

A informação somente deve ser acessada pelo usuário previamente autorizado e que necessita obter a informação para realizar suas atividades profissionais relacionadas à organização.

Segundo o Tribunal de Contas da União, a Confidencialidade (Brasil, TCU, 2012, página 9):

"Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento."

Integridade

A informação deve ser mantida no seu estado original, a informação não deve ser corrompida ao longo do tempo.

Segundo o Tribunal de Contas da União, a integridade (Brasil, TCU, 2012, página 9):

"Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados."

Disponibilidade

A informação deve estar disponível para as atividades da organização. Segundo o Tribunal de Contas da União, a autenticidade (Brasil, TCU, 2012, página 10):

"Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito."

Autenticidade

A origem da informação deve ser possível de ser identificada. Segundo o Tribunal de Contas da União, a autenticidade (Brasil, TCU, 2012, página 9):

"Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações."

Auditabilidade

O uso da informação deve ter condições de ser auditado.

As ações que utilizam a informação devem ser registradas.

Legalidade

O uso da informação e dos recursos de informação deve estar de acordo com a legislação vigente, com as regras corporativas, com as exigências contratuais e com os demais regulamentos e **normativos** com os quais a organização precisa estar em conformidade.

Normativos:
São as normas brasileiras definidas pela ABNT e as normas internacionais definidas pela ISO/IEC.

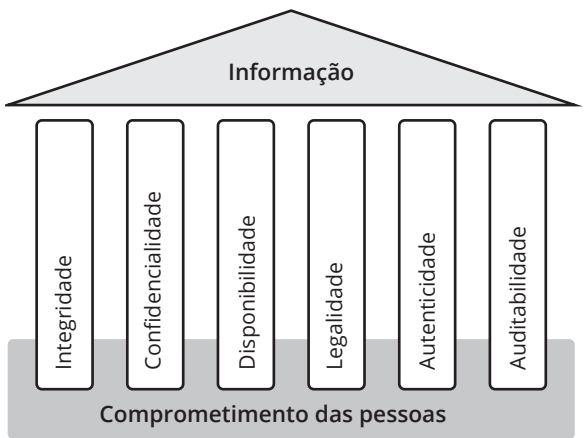


Figura 1.1
Objetivos da Segurança da Informação.

Exercício de fixação
Confidencialidade, integridade, disponibilidade, legalidade, autenticidade e auditabilidade

A disponibilidade, integridade, confidencialidade, autenticidade, legalidade e auditabilidade possuem a mesma importância. Porém, em alguns momentos um desses objetivos de segurança da informação fica mais relevante. Nas situações a seguir, indique qual delas é mais relevante para o momento específico.

a. Recuperação da Caixa Preta do avião AF-447 da Air France, que caiu no Oceano Atlântico.

b. Em relação também à caixa preta, mas em um momento anterior à queda do avião, quando o voo prosseguia sem problemas e os comandantes conversavam normalmente e trocavam informações com os controladores do tráfego aéreo.

c. Quando o eleitor se apresenta na sala para votar.

d. Quando o eleitor se dirige à cabine de votação para realizar o seu voto.

Para que o Processo Organizacional de Segurança da Informação seja desenvolvido, implantado e mantido, é necessário que exista uma estruturação de como este processo deve acontecer. O processo deve ser o mesmo para informações físicas e informações lógicas.

A Norma *ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação – Requisitos e a Norma ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação* são as normas básicas sobre o assunto e descrevem uma família de controles que devem ser considerados para a existência do Processo Organizacional de Segurança da Informação. Esses controles podem ser agrupados em **Dimensões da Segurança da Informação**.

Dimensões da Segurança da Informação: São os aspectos que devem ser considerados em um Processo de Segurança da Informação, considerando a Família NBR ISO/IEC 27000 de normas de segurança da informação.

Uma Dimensão da Segurança da Informação é um conjunto de controles que parte de uma mesma disciplina de segurança, que podem ser tratados da mesma maneira e sob uma mesma gestão.

O quadro a seguir ilustra as Dimensões da Segurança da Informação:

Processo Corporativo de Segurança da Informação

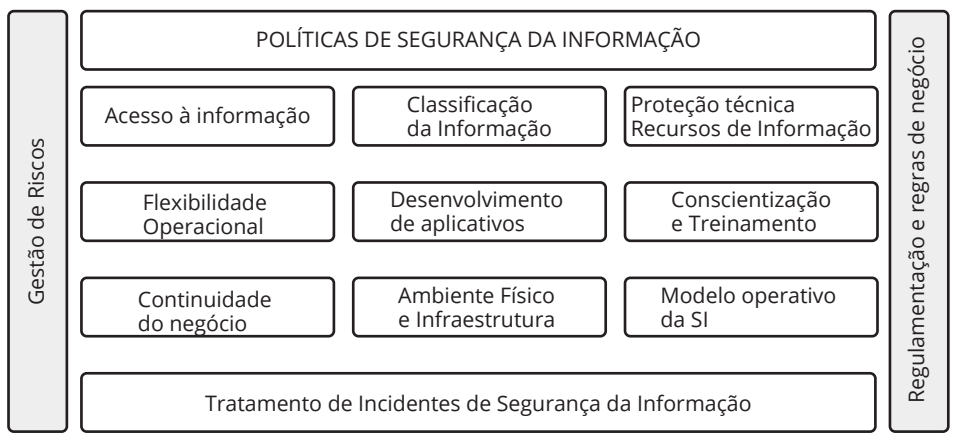


Figura 1.2 Dimensões da Segurança da Informação. Estrutura baseada na Norma Internacional ISO/IEC 27002.

Descrevemos a seguir o objetivo de cada Dimensão da Segurança da Informação. A importância de cada dimensão é igual para todo o Processo Organizacional de Segurança da Informação. Não existe uma dimensão mais importante do que outra. A maturidade da organização em Segurança da Informação valerá pela eficiência e efetividade do conjunto de dimensões.

Será pouco efetivo se uma dimensão estiver em um patamar de excelência e em outra dimensão estiver um caos. Semelhante a uma corrente, a proteção da informação será quebrada no seu elemento mais frágil.

Gestão de Risco

Definir, implantar e manter a Gestão de Riscos de Segurança da Informação para a existência de um monitoramento e tratamento das ameaças que podem gerar impactos financeiros, impactos de imagem, impacto operacional ou qualquer outro impacto nos recursos de informação que possa comprometer as atividades e os objetivos da organização.

Políticas de Segurança da Informação

Desenvolver, implantar e manter atualizados os regulamentos necessários para que a organização possua um efetivo processo de segurança da informação. Esses regulamentos definem como a organização deseja que a informação seja utilizada, controlada, tenha seu uso responsabilizado e esteja em conformidade com a legislação e demais regras que a organização necessite cumprir.

Acesso à informação

Garantir o adequado acesso à informação, definindo regras e responsabilidades para:

- O seu uso;
- Autorização de acesso pelo usuário;
- Tipos de usuários contemplados;
- Tipos de acesso;
- Possibilidade de auditar o acesso;
- Consultas sobre acessos realizados ou potenciais acessos.

Classificação da informação

Definir o padrão de sigilo que será utilizado para a informação da organização e classificar cada informação em relação a esse padrão.

Proteção técnica de recursos de informação

Garantir a existência de uma gestão técnica para os recursos de tecnologia da informação da organização. Deve-se também garantir a continua atualização das medidas de proteção da informação.

Flexibilidade operacional

Garantir a existência e a efetividade da Gestão de Mudanças, Gestão de Problemas, Gestão de Ativos e Gestão de Capacidade para os recursos de informação.

Desenvolvimento ou aquisição de sistemas

Garantir que para o desenvolvimento ou aquisição de sistemas aplicativos sejam considerados e cumpridos os requisitos de segurança relacionados ao desenvolvimento dos programas, a manutenção dos programas, a dependência dos desenvolvedores (internos ou externos) e a continuidade da existência desse aplicativo ao longo do tempo.

Conscientização e treinamento de usuário

Desenvolver atividades de conscientização e treinamento de usuários em segurança da informação. Deve-se considerar todo tipo de usuário que utilizará a informação da organização.

Continuidade de negócio

Garantir a continuidade do negócio, no que depende da informação e dos recursos de informação, quando de uma ocorrência de uma indisponibilidade da informação.

Ambiente físico e infraestrutura

Garantir a proteção do ambiente físico onde existam recursos de informação, bem como garantir a existência de infraestrutura para que a informação possa ser utilizada pela organização.

Modelo operativo da Segurança da Informação

Definir, implantar e monitorar a estrutura organizacional da Segurança da Informação: formação, responsabilidades, hierarquia, relacionamento com outras áreas organizacionais, relacionamento com entidades externas e relacionamento com autoridades do governo.

Tratamento de incidentes

Garantir a existência de uma gestão de incidentes de segurança da informação. Incidente é qualquer acontecimento que não esteja adequado às definições e controles de segurança da informação. Segundo a Norma NBR ISO/IEC 27001, "incidente de segurança da informação é um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação".

Exercício de fixação
Dimensões de segurança

Considerando as Dimensões da Segurança da Informação, como você considera a maturidade da sua organização em cada uma delas? Ruim, regular ou boa?

- **Ruim:** não existem os controles ou os controles existentes não são efetivos. É urgente a implantação de controles para a existência da dimensão de segurança;
- **Regular:** existem alguns controles e atendem o mínimo para a segurança da informação. Considerando o tipo da organização, é necessário melhorar ou complementar esses controles;
- **Boa:** existem controles que garantem a existência de uma efetiva dimensão da segurança da informação. Pequenas melhorias são necessárias.

Justifique.

Dimensão Política de Segurança da Informação

A Dimensão Política de Segurança da Informação tem por objetivo desenvolver, implantar e manter atualizados os regulamentos necessários para que a organização possua um efetivo processo de segurança da informação. Esses regulamentos definem como a organização deseja que a informação seja utilizada, controlada e tenha seu uso responsabilizado.

Essa dimensão tem uma característica específica que a diferencia das demais dimensões de segurança da informação. A Dimensão Política de Segurança da Informação define a regulamentação de todas as demais dimensões. Isto é, essa dimensão é uma base para todas as ações que serão necessárias para um efetivo Processo Organizacional de Segurança da Informação.

A Dimensão Política de Segurança da Informação definirá para cada outra dimensão:

- Os controles que devem ser considerados;
- O escopo (abrangência) que deve ser considerado;
- As responsabilidades dos usuários, gestores e demais pessoas pelo desenvolvimento, implantação e manutenção dos controles;
- A estrutura e regras para as revisões dos controles;
- Tudo mais que precise ser regulamentado para que a dimensão exista com sucesso.

É preciso entender que a Dimensão Política de Segurança da Informação, ao desenvolver regulamentos para uma dimensão, não realizará as ações necessárias desta outra dimensão. Por exemplo, existirá um regulamento para a Dimensão de Continuidade de Negócio que indicará que "a organização deve ter planos para situações de indisponibilidade da informação de maneira que a organização e o seu negócio tenha apenas um pequeno impacto. Os Diretores de Área são os responsáveis para avaliar e indicar o tempo máximo de indisponibilidade dos recursos de informação".

Nesse exemplo, esse regulamento indica que a organização deseja que existam planos de continuidade de negócio para quando ocorrerem situações de indisponibilidade da informação. Também define uma responsabilidade para os Diretores de Área. Sendo assim, esse regulamento indica como deve ser o tratamento para situações de indisponibilidade da informação. Esse regulamento é um orientador oficial, um balizador oficial como devem acontecer as ações de continuidade de negócio. Porém, o Plano de Continuidade de Negócio será desenvolvido, implantado e mantido pela Dimensão de Continuidade de Negócio.

Os regulamentos gerados pela Dimensão Política de Segurança da Informação orientarão e facilitarão como as demais dimensões devem acontecer.

A Dimensão Política de Segurança da Informação é considerada uma dimensão estrutural. É conveniente que existam os regulamentos de segurança da informação para que os controles de cada dimensão sejam definidos, explicitados, implantados e mantidos.

O Tribunal de Contas da União define a política de segurança da informação (Brasil, TCU, 2012, página 10):

"Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações."

Política de segurança da informação como elemento de estruturas teóricas

A política de segurança da informação aparece como elemento em diversas estruturas teóricas relacionadas à informação e à tecnologia da informação. Descrevemos a seguir o seu relacionamento com algumas dessas principais estruturas.

Política de segurança da informação e a norma 'ABNT NBR ISO/IEC 27002:2013 – tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação'

A *ABNT NBR ISO/IEC 27002:2013* é a norma básica para o Processo Organizacional de Segurança da Informação no que diz respeito aos controles que devem ser considerados para esse processo. Todas as outras normas da Família 27000 e outras normas relacionadas à segurança da informação devem ser consideradas, porém essa norma é a estrutura para a construção dos artefatos que vão compor a segurança da informação.

O Tribunal de Contas da União afirma no seu *Manual de Boas Práticas de Segurança da Informação*, no capítulo 4, *TCU e a ABNT NBR ISO/IEC 27002*, que essa é a norma técnica de auditoria de segurança da informação utilizada pelo TCU (Brasil, TCU, 2012, página 38). Essa afirmação respalda a Norma *ABNT NBR ISO/IEC 27002* como o guia básico para a organização definir, desenvolver, implantar e manter o Processo Organizacional de Segurança da Informação.

O objetivo da NBR ISO/IEC 27002:2013 é declarado da seguinte forma (ABNT, 2013, página 1):

"Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização."

Para a implantação da segurança da informação na organização, a norma já cita no seu início a necessidade da existência da política em conjunto com os processos e procedimentos (ABNT, 2013, página x).

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

A *NBR ISO/IEC 27002:2013* é composta por 19 capítulos, numerados de 0 a 18. Distribuídos nesses capítulos estão os 114 controles que devem ser considerados para as Dimensões da Segurança da Informação.

A Dimensão Política de Segurança da Informação deve contemplar esses controles para o desenvolvimento, implantação e manutenção dos regulamentos que vão compor o Processo Organizacional de Segurança da Informação.

O capítulo 5 dessa norma trata da Dimensão Política de Segurança da Informação e recomenda que o documento a ser desenvolvido defina como a organização quer que o assunto seja tratado, identifique as responsabilidades, oriente sobre a comunicação para as pessoas e garanta que o Processo Organizacional de Segurança da Informação seja eficiente e eficaz ao longo do tempo.

Porém nem nesse capítulo, nem em outro capítulo dessa norma, nem em outro normativo existe a descrição de como deve ser construído o documento de política de segurança da informação ou como deve ser estruturado. Essa orientação é o objetivo deste curso.

A descrição detalhada dos controles, as orientações e as considerações sobre a sua implantação e manutenção encontram-se descritos na norma que deve ser estudada no seu texto completo e sempre tomada como base. Quando ocorrer a implantação do Processo Organizacional de Segurança da Informação, a norma deve ser consultada.

Listamos a seguir apenas os controles que, descritos em cada capítulo da norma, devem ser considerados quando ocorrer a elaboração dos documentos que vão compor a política de segurança da informação da organização.

Controles de Segurança da Informação – NBR ISO/IEC 27002:2013

Capítulo 5 – Políticas de segurança da informação

(1) Controle: Políticas para a segurança da informação.

5.1.1 – Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes (ABNT, NBR 27002, 2013, página 2).

(2) Controle: Análise crítica das políticas de segurança da informação.

5.1.2 – Convém que as políticas de segurança da informação sejam analisadas criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia (ABNT, NBR 27002, 2013, página 4).

Capítulo 6 – Organização da segurança da informação

(3) Controle: Responsabilidades e papéis pela segurança da informação.

6.1.1 – Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas (ABNT, NBR 27002, 2013, página 4).

(4) Controle: Segregação de funções.

6.1.2 – Convém que funções conflitantes e áreas de responsabilidades sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização (ABNT, NBR 27002, 2013, página 5).

(5) Controle: Contato com autoridades.

6.1.3 – Convém que contatos apropriados com autoridades relevantes sejam mantidos (ABNT, NBR 27002, 2013, página 6).

(6) Controle: Contato com grupos especiais.

6.1.4 – Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos (ABNT, NBR 27002, 2013, página 6).

(7) Controle: Segurança da informação no gerenciamento de projetos.

6.1.5 – Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto (ABNT, NBR 27002, 2013, página 7).

(8) Controle: Política para uso de dispositivo móvel.

6.2.1 – Convém que uma política e medidas que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis (ABNT, NBR 27002, 2013, página 8).

(9) Controle: Trabalho remoto.

6.2.2 – Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto (ABNT, NBR 27002, 2013, página 9).

Capítulo 7 – Segurança em recursos humanos

(10) Controle: Recursos Humanos – Seleção.

7.1.1 – Convém que verificações do histórico sejam realizadas para todos os candidatos a empregos, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos de negócio, aos riscos percebidos e à classificação das informações a serem acessadas (ABNT, NBR 27002, 2013, página 11).

(11) Controle: Recursos Humanos – Termos e condições de contratação.

7.1.2 – Convém que as obrigações contratuais com funcionários e partes externas declarem a sua responsabilidade e as da organização para a segurança da informação (ABNT, NBR 27002, 2013, página 12).

(12) Controle: Recursos Humanos – Responsabilidade da Direção.

7.2.1 – Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização (ABNT, NBR 27002, 2013, página 13).

(13) Controle: Recursos Humanos – Conscientização, educação e treinamento.

7.2.2 – Convém que todos os funcionários da organização e, onde pertinente, partes externas, recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções (ABNT, NBR 27002, 2013, página 13).

(14) Controle: Recursos Humanos – Processo disciplinar.

7.2.3 – Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação da segurança da informação (ABNT, NBR 27002, 2013, página 15).

(15) Controle: Recursos Humanos – Encerramento ou mudança de contratação.

7.3.1 – Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação sejam definidas, comunicadas aos funcionários ou partes externas e cumpridas (ABNT, NBR 27002, 2013, página 16).

Capítulo 8 – Gestão de ativos

(16) Controle: Inventário dos ativos.

8.1.1 – Convém que os ativos associados à informação e aos recursos de processamento da informação sejam identificados, e um inventário destes ativos seja estruturado e mantido (ABNT, NBR 27002, 2013, página 16).

(17) Controle: Proprietário dos ativos.

8.1.2 – Convém que os ativos mantidos no inventário tenham um proprietário (ABNT, NBR 27002, 2013, página 17).

(18) Controle: Uso aceitável dos ativos.

8.1.3 – Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação sejam identificadas, documentadas e implementadas (ABNT, NBR 27002, 2013, página 18).

(19) Controle: Devolução de ativos.

8.1.4 – Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou do acordo (ABNT, NBR 27002, 2013, página 18).

(20) Controle: Classificação da informação.

8.2.1 – Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada (ABNT, NBR 27002, 2013, página 18).

(21) Controle: Rótulos e tratamento da informação.

8.2.2 – Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação adotado pela organização (ABNT, NBR 27002, 2013, página 20).

(22) Controle: Tratamento dos ativos

8.2.3 – Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização (ABNT, NBR 27002, 2013, página 20).

(23) Controle: Gerenciamento de mídias removíveis.

8.3.1 – Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização (ABNT, NBR 27002, 2013, página 21).

(24) Controle: Descarte de mídias

8.3.2 – Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais (ABNT, NBR 27002, 2013, página 22).

(25) Controle: Transferência física de mídias.

8.3.3 – Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção durante o transporte (ABNT, NBR 27002, 2013, página 22).

Capítulo 9 – Controle de acesso

(26) Controle: Política de controle de acesso.

9.1.1 – Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios (ABNT, NBR 27002, 2013, página 23).

(27) Controle: Acesso às redes e aos serviços de rede.

9.1.2 – Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados para utilizar (ABNT, NBR 27002, 2013, página 25).

(28) Controle: Registro e cancelamento de usuário.

9.2.1 – Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição dos direitos de acesso (ABNT, NBR 27002, 2013, página 25).

(29) Controle: Provisionamento para acesso de usuário.

9.2.2 – Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços (ABNT, NBR 27002, 2013, página 26).

(30) Controle: Gerenciamento de direitos de acesso privilegiados.

9.2.3 – Convém que a concessão e o uso de direitos de acesso privilegiado sejam restritos e controlados (ABNT, NBR 27002, 2013, página 27).

(31) Controle: Gerenciamento da informação de autenticação secreta de usuários.

9.2.4 – Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal (ABNT, NBR 27002, 2013, página 28).

(32) Controle: Análise crítica dos direitos de acesso de usuário.

9.2.5 – Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários a intervalos regulares (ABNT, NBR 27002, 2013, página 28).

(33) Controle: Retirada ou ajuste dos direitos de acesso.

9.2.6 – Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança desta atividade (ABNT, NBR 27002, 2013, página 29).

(34) Controle: Uso da informação de autenticação secreta.

9.3.1 – Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta (ABNT, NBR 27002, 2013, página 30).

(35) Controle: Restrição de acesso à informação.

9.4.1 – Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso (ABNT, NBR 27002, 2013, página 31).

(36) Controle: Procedimentos seguros de entrada no sistema (log-on).

9.4.2 – Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (log-on) (ABNT, NBR 27002, 2013, página 31).

(37) Controle: Sistemas de gerenciamento de senha.

9.4.3 – Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade (ABNT, NBR 27002, 2013, página 33).

(38) Controle: Uso de programas utilitários privilegiados.

9.4.4 – Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado (ABNT, NBR 27002, 2013, página 33).

(39) Controle: Controle de acesso ao código fonte de programas.

9.4.5 – Convém que o acesso ao código fonte de programas seja restrito (ABNT, NBR 27002, 2013, página 34).

Capítulo 10 – Criptografia

(40) Controle: Política para uso de controles criptográficos.

10.1.1 – Convém que seja desenvolvida e implementada uma política sobre o uso de controles criptográficos para a proteção da informação (ABNT, NBR 27002, 2013, página 35).

(41) Controle: Gerenciamento de chaves.

10.1.2 – Convém que uma política sobre o uso, proteção e tempo de vida das chaves criptográficas seja desenvolvida e implementada ao longo de todo o seu ciclo de vida (ABNT, NBR 27002, 2013, página 36).

Capítulo 11 – Segurança física e do ambiente

(42) Controle: Perímetro de segurança física.

11.1.1 – Convém que perímetros de segurança sejam definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis (ABNT, NBR 27002, 2013, página 38).

(43) Controle: Controles de entrada física.

11.1.2 – Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido (ABNT, NBR 27002, 2013, página 39).

(44) Controle: Segurança em escritórios, salas e instalações.

11.1.3 – Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações (ABNT, NBR 27002, 2013, página 40).

(45) Controle: Proteção contra ameaças externas e do meio ambiente.

11.1.4 – Convém que seja projetada e aplicada proteção física contra desastres naturais, ataques maliciosos ou acidentes (ABNT, NBR 27002, 2013, página 40).

(46) Controle: Trabalhando em áreas seguras.

11.1.5 – Convém que sejam projetados e aplicados procedimentos para o trabalho em áreas seguras (ABNT, NBR 27002, 2013, página 40).

(47) Controle: Áreas de entrega e de carregamento.

11.1.6 – Convém que pontos de acesso como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações sejam controlados e, se possível, isolados das instalações de processamento de informação, para evitar o acesso não autorizado (ABNT, NBR 27002, 2013, página 41).

(48) Controle: Localização e proteção do equipamento.

11.2.1 – Convém que os equipamentos sejam protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado (ABNT, NBR 27002, 2013, página 41).

(49) Controle: Utilidades.

11.2.2 – Convém que os equipamentos sejam protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas das utilidades (ABNT, NBR 27002, 2013, página 42).

(50) Controle: Segurança do cabeamento.

11.2.3 – Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos (ABNT, NBR 27002, 2013, página 43).

(51) Controle: Manutenção dos equipamentos.

11.2.4 – Convém que os equipamentos tenham uma manutenção correta para assegurar a sua contínua integridade e disponibilidade (ABNT, NBR 27002, 2013, página 43).

(52) Controle: Remoção de ativos.

11.2.5 – Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia (ABNT, NBR 27002, 2013, página 44).

(53) Controle: Segurança de equipamentos e ativos fora das dependências da organização.

11.2.6 – Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização (ABNT, NBR 27002, 2013, página 45).

(54) Controle: Reutilização ou descarte seguro de equipamentos.

11.2.7 – Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes da reutilização, para assegurar que todos os dados sensíveis e software licenciados tenham sido removidos ou sobregravados com segurança (ABNT, NBR 27002, 2013, página 46).

(55) Controle: Equipamento de usuário sem monitoração.

11.2.8 – Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada (ABNT, NBR 27002, 2013, página 46).

(56) Controle: Política de mesa limpa e tela limpa.

11.2.9 – Convém que sejam adotadas uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento de informação (ABNT, NBR 27002, 2013, página 47).

Capítulo 12 – Segurança nas operações

(57) Controle: Documentação dos procedimentos de operação.

12.1.1 – Convém que os procedimentos de operação sejam documentados e disponibilizados para todos os usuários que necessitem deles (ABNT, NBR 27002, 2013, página 48).

(58) Controle: Gestão de mudanças.

12.1.2 – Convém que mudanças na organização, nos processos de negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas (ABNT, NBR 27002, 2013, página 49).

(59) Controle: Gestão de capacidade.

12.1.3 – Convém que a utilização dos recursos seja monitorada e ajustada, e que as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema (ABNT, NBR 27002, 2013, página 49).

(60) Controle: Separação dos ambientes de desenvolvimento, teste e produção.

12.1.4 – Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção (ABNT, NBR 27002, 2013, página 50).

(61) Controle: Controles contra malware.

12.2.1 – Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário (ABNT, NBR 27002, 2013, página 51).

(62) Controle: Cópias de segurança das informações.

12.3.1 – Convém que cópias de segurança das informações, dos software e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida (ABNT, NBR 27002, 2013, página 53).

(63) Controle: Registro de eventos.

12.4.1 – Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares (ABNT, NBR 27002, 2013, página 54).

(64) Controle: Proteção das informações dos registros de eventos (log).

12.4.2 – Convém que as informações dos registros de eventos (log) e os seus recursos sejam protegidos contra acesso não autorizado e adulteração (ABNT, NBR 27002, 2013, página 55).

(65) Controle: Registro de eventos (log) de administrador e operador.

12.4.3 – Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (log) protegidos e analisados criticamente, a intervalos regulares (ABNT, NBR 27002, 2013, página 56).

(66) Controle: Sincronização dos relógios.

12.4.4 – Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa (ABNT, NBR 27002, 2013, página 56).

(67) Controle: Instalação de software nos Sistemas Operacionais.

12.5.1 – Convém que procedimentos para controlar a instalação de software em Sistemas Operacionais sejam implementados (ABNT, NBR 27002, 2013, página 57).

(68) Controle: Gestão de vulnerabilidades técnicas.

12.6.1 – Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas em tempo hábil; convém que a exposição da organização a estas vulnerabilidades seja avaliada e que sejam tomadas as medidas apropriadas para lidar com os riscos associados (ABNT, NBR 27002, 2013, página 58).

(69) Controle: Restrição quanto à instalação de software.

12.6.2 – Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários (ABNT, NBR 27002, 2013, página 59).

(70) Controle: Controles de auditoria de sistemas de informação.

12.7.1 – Convém que as atividades e requisitos de auditoria envolvendo a verificação nos Sistemas Operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio (ABNT, NBR 27002, 2013, página 60).

Capítulo 13 – Segurança nas comunicações

(71) Controle: Controles de redes

13.1.1 – Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações (ABNT, NBR 27002, 2013, página 61).

(72) Controle: Segurança dos serviços de rede.

13.1.2 – Convém que mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados (ABNT, NBR 27002, 2013, página 61).

(73) Controle: Segregação de redes.

13.1.3 – Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes (ABNT, NBR 27002, 2013, página 62).

(74) Controle: Políticas e procedimentos para transferência de informações.

13.2.1 – Convém que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações, por meio de uso de todos os tipos de recursos de comunicação (ABNT, NBR 27002, 2013, página 63).

(75) Controle: Acordos para transferência de informações.

13.2.2 – Convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e as partes externas (ABNT, NBR 27002, 2013, página 64).

(76) Controle: Mensagens eletrônicas.

13.2.3 – Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas (ABNT, NBR 27002, 2013, página 65).

(77) Controle: Acordos de confidencialidade e não divulgação.

13.2.4 – Convém que os requisitos para a confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados (ABNT, NBR 27002, 2013, página 668).

Capítulo 14 – Aquisição, desenvolvimento e manutenção de sistemas

(78) Controle: Análise e especificação dos requisitos de segurança da informação.

14.1.1 – Convém que os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes (ABNT, NBR 27002, 2013, página 67).

(79) Controle: Serviços de aplicação seguros em redes públicas.

14.1.2 – Convém que as informações envolvidas nos serviços de aplicação que transitam sobre as redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas (ABNT, NBR 27002, 2013, página 68).

(80) Controle: Protegendo as transações nos aplicativos de serviços.

14.1.3 – Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada (ABNT, NBR 27002, 2013, página 70).

(81) Controle: Política de desenvolvimento seguro.

14.2.1 – Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização (ABNT, NBR 27002, 2013, página 70).

(82) Controle: Procedimentos para controle de mudança de sistemas.

14.2.2 – Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças (ABNT, NBR 27002, 2013, página 71).

(83) Controle: Análise crítica técnica das aplicações após mudanças nas plataformas operacionais.

14.2.3 – Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para garantir que não haverá qualquer impacto adverso na operação da organização ou na segurança (ABNT, NBR 27002, 2013, página 73).

(84) Controle: Restrições sobre mudanças em pacotes de software.

14.2.4 – Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas (ABNT, NBR 27002, 2013, página 73).

(85) Controle: Princípios para projetar sistemas seguros.

14.2.5 – Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação (ABNT, NBR 27002, 2013, página 74).

(86) Controle: Ambiente seguro para desenvolvimento.

14.2.6 – Convém que as organizações estabeleçam e protejam adequadamente ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema (ABNT, NBR 27002, 2013, página 74).

(87) Controle: Desenvolvimento terceirizado.

14.2.7 – Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado (ABNT, NBR 27002, 2013, página 75).

(88) Controle: Testes de segurança do sistema.

14.2.8 – Convém que os testes das funcionalidades de segurança sejam realizados durante o desenvolvimento e sistemas (ABNT, NBR 27002, 2013, página 76).

(89) Controle: Teste de aceitação de sistemas.

14.2.9 – Convém que testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões (ABNT, NBR 27002, 2013, página 76).

(90) Controle: Proteção dos dados para testes.

14.3.1 – Convém que os dados de testes sejam selecionados com cuidado, protegidos e controlados (ABNT, NBR 27002, 2013, página 76).

Capítulo 15 – Relacionamento na cadeia de suprimento

(91) Controle: Política de segurança da informação no relacionamento com os fornecedores.

15.1.1 – Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados (ABNT, NBR 27002, 2013, página 77).

(92) Controle: Identificando segurança da informação nos acordos com fornecedores

15.1.2 – Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização, (ABNT, NBR 27002, 2013, página 78).

(93) Controle: Cadeia de suprimento na tecnologia da informação e comunicação.

15.1.3 – Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados à cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação (ABNT, NBR 27002, 2013, página 80).

(94) Controle: Monitoramento e análise crítica de serviços com fornecedores.

15.2.1 – Convém que as organizações monitorem, analisem criticamente e auditem, a intervalos regulares, a entrega dos serviços executados pelos fornecedores (ABNT, NBR 27002, 2013, página 81).

(95) Controle: Gerenciamento de mudanças para serviços com fornecedores.

15.2.2 – Convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação de riscos. (ABNT, NBR 27002, 2013, página 82).

Capítulo 16 – Gestão de incidentes de segurança da informação

(96) Controle: Responsabilidad es e procedimentos.

16.1.1 – Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação. (ABNT, NBR 27002, 2013, página 83).

(97) Controle: Notificação de eventos de segurança da informação.

16.1.2 – Convém que os eventos de segurança da informação sejam relatados por meio de canais de gestão, o mais rapidamente possível (ABNT, NBR 27002, 2013, página 84).

(98) Controle: Notificando fragilidades de segurança da informação.

16.1.3 – Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização sejam instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços (ABNT, NBR 27002, 2013, página 85).

(99) Controle: Avaliação e decisão dos eventos de segurança da informação.

16.1.4 – Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação (ABNT, NBR 27002, 2013, página 86).

(100) Controle: Resposta aos incidentes de segurança da informação.

16.1.5 – Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados (ABNT, NBR 27002, 2013, página 86).

(101) Controle: Aprendendo com os incidentes de segurança da informação.

16.1.6 – Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros (ABNT, NBR 27002, 2013, página 87).

(102) Controle: Coleta de evidências.

16.1.7 – Convém que a organização defina e aplique procedimentos para identificação, coleta, aquisição e preservação dos informações, as quais podem servir como evidências (ABNT, NBR 27002, 2013, página 87).

Capítulo 17 – Aspectos de segurança da informação na gestão de continuidade do negócio

(103) Controle: Planejando a continuidade da segurança da informação.

17.1.1 – Convém que a organização determine seus requisitos para a segurança da informação e continuidade da gestão da segurança da informação em situações diversas, por exemplo, durante uma crise ou desastre (ABNT, NBR 27002, 2013, página 88).

(104) Controle: Implementando a continuidade da segurança da informação.

17.1.2 – Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa (ABNT, NBR 27002, 2013, página 89).

(105) Controle: Verificação, análise crítica e avaliação da continuidade da segurança da informação.

17.1.3 – Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles sejam válidos e eficazes em situações adversas (ABNT, NBR 27002, 2013, página 90).

(106) Controle: Disponibilidade dos recursos de processamento da informação.

17.2.1 – Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade. (ABNT, NBR 27002, 2013, página 91).

Capítulo 18 – Conformidade

(107) Controle: Identificação da legislação aplicável e de requisitos contratuais

18.1.1 – Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes e o enfoque da organização para atender a esses requisitos sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização (ABNT, NBR 27002, 2013, página 91).

(108) Controle: Direitos de propriedade intelectual.

18.1.2 – Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados aos direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários (ABNT, NBR 27002, 2013, página 93).

(109) Controle: Proteção de registros.

18.1.3 – Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio (ABNT, NBR 27002, 2013, página 93).

(110) Controle: Proteção e privacidade de informações de identificação pessoal.

18.1.4 – Convém que a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável (ABNT, NBR 27002, 2013, página 94).

(111) Controle: Regulamentação de controles de criptografia.

18.1.5 – Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentação pertinentes (ABNT, NBR 27002, 2013, página 94).

(112) Controle: Análise crítica independente da segurança da informação.

18.2.1 – Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivo dos controles, controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas (ABNT, NBR 27002, 2013, página 95).

(113) Controle: Conformidade com as políticas e procedimentos de segurança da informação.

18.2.2 – Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidades, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação (ABNT, NBR 27002, 2013, página 96).

(114) Controle: Análise crítica da conformidade técnica.

18.2.3 – Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização (ABNT, NBR 27002, 2013, página 96).

Política de segurança da informação e a Norma 'NBR ISO/IEC 27001:2013 – tecnologia da informação – técnicas de segurança – sistema de gestão de segurança da informação – requisitos'

Essa norma define um modelo que estabelece, implanta, opera, monitora, analisa criticamente, mantém e melhora o Sistema de Gestão de Segurança da Informação (SGSI).
Ela também pode ser utilizada por partes internas e externas para avaliar a conformidade com os controles definidos na Norma *ABNT NBR ISO/IEC 27002* e no caso de parte externa, possibilitar a certificação da organização em segurança da informação.

A política de segurança da informação é um dos controles que deve ser considerado. Ela é um controle básico, pois nela são declarados os demais controles, em maior ou menor nível de granularidade, que serão considerados pela organização.

Esta norma considera a política de segurança da informação como elemento de responsabilidade da Alta Direção:

"5 Liderança

5.1 – Liderança e comprometimento

A Alta Direção deve demonstrar a sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a. assegurando que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização; (ABNT, NBR 27001, 2013, página 2)."

Sendo a Alta Direção responsável pela existência da política de segurança da informação, essa norma complementa:

"5.2 Política

A Alta Direção deve estabelecer uma política de segurança da informação que:

a. seja apropriada ao propósito da organização;
b. inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação;
c. inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;
d. inclua o comprometimento com a melhoria continua do sistema de gestão da segurança da informação; (ABNT, NBR 27001, 2013, página 3).

A política se segurança da informação deve:

a. estar disponível como informação documentada;
b. ser comunicada dentro da organização;
c. estar disponível para as partes interessadas, conforme apropriado (ABNT, NBR 27001, 2013, página 3)."

A norma considera a política de segurança da informação um elemento importante, que se confirma quando a norma declara:

"6.2 – Objetivo de segurança da informação e planejamento para alcançá-los.

A organização deve estabelecer os objetivos de segurança da informação para as funções e níveis relevantes.

Os objetivos de segurança da informação devem:

a. ser consistentes com a política de segurança da informação;
b. ser mensuráveis (quando aplicável);
c. levar em conta os requisitos de segurança da informação aplicáveis e os resultados da avaliação e tratamento de riscos;
d. ser comunicados; e
e. ser atualizado, conforme apropriado.

(ABNT, NBR 27001, 2013, página 5)."

Quando a norma trata da conscientização, a política de segurança da informação é novamente citada:

"7. Apoio

7.3 – Conscientização

Pessoas que realizam trabalhos sob o controle da organização devem estar cientes da:

a. política de segurança da informação;
b. suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e
c. implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação (ABNT, NBR 27001, 2013, página 6)."

No final, de uma maneira indireta, essa norma indica a melhoria da política de segurança da informação, quando indica:

"10.2 Melhoria contínua

A organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação

(ABNT, NBR 27001, 2013, página 11)."

Política de segurança da informação e a norma NBR ISO/IEC 27005:2008 – tecnologia da informação – técnicas de segurança – gestão de riscos de segurança da informação

Essa norma define as diretrizes para o processo de Gestão de Riscos em Segurança da Informação atendendo aos requisitos de um SGSI, de acordo com a ABNT NBR ISO/IEC 27001. Nessa norma é feito um relacionamento do escopo do SGSI com a Dimensão Política de Segurança da Informação e com a Dimensão Gestão de Riscos.

Na Dimensão da Gestão de Riscos, a política de segurança da informação é considerada na fase de definição do contexto, do escopo e dos limites.

No Capítulo 7 – Definição de contexto, no item 7.3 – Escopo e limites, essa norma declara que "convém que a organização defina o escopo e os limites da gestão de riscos de segurança da informação" (ABNT, 2008, página 8).

Para a definição do escopo e limites a, norma ISO/IEC 27005 cita a Política de Segurança da Informação quando declara no item 7.3 – Escopo e limites:

Ao definir escopo e limites, convém que a organização considere as seguintes informações:

- Os objetivos estratégicos, políticas e estratégias da organização;
- Processo de negócio;
- As funções e estrutura da organização;
- Requisitos legais, regulatórios e contratuais aplicáveis à organização;
- *A política de segurança da informação* (grifo nosso);
- A abordagem da organização à gestão de riscos;
- Ativos de informação;
- Localidades em que a organização se encontra e características geográficas;
- Restrições que afetam a organização;
- Expectativas das partes interessadas;
- Ambiente sociocultural;
- Interfaces (ou seja, a troca de informação com o ambiente).

Em seguida, a norma complementa:

"O escopo e os limites da gestão de riscos de segurança da informação estão relacionados ao escopo e aos limites do SGSI, conforme requerido na ABNT ISO/IEC 27001 4.2.1.a (ABNT, 2008, página 9)."

A gestão de riscos é parte do Sistema de Gestão de Segurança da Informação e fará com que este SGSI se mantenha contínuo:

"Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um SGSI (ABNT, 2008, página 3)."

A NBR ISO/IEC 27001:2006 relaciona no item 4.2.1 – Estabelecer o SGSI, os elementos necessários para que a organização estabeleça um SGSI. A Segurança da Informação aparece como um dos elementos:

a. Definir o escopo e os limites do SGSI (Sistema de Gestão de Segurança da Informação) nos termos das características do negócio, a organização, sua localização, ativos de tecnologia, incluindo detalhes para quaisquer exclusões do escopo.

b. Definir uma política do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia que:

1. inclua uma estrutura para definir objetivos e estabeleça um direcionamento global e princípios para as ações relacionadas com a segurança da informação;
2. considere os requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;
3. esteja alinhada com o contexto estratégico de gestão de risco da organização no qual o estabelecimento e manutenção do SGSI irá ocorrer;
4. estabeleça critérios em relação aos quais os riscos serão avaliados.

c. Definir a abordagem de análise e avaliação de riscos da organização.

(ABNT, 2006, páginas 4-5)

d. Identificar os riscos.

e. Analisar e avaliar os riscos.

f. Identificar e avaliar as opções para o tratamento de risco.

g. Selecionar objetivos de controle e controles para o tratamento de riscos.

h. Obter aprovação da direção dos riscos residuais propostos.

i. Obter autorização da direção para implementar e operar o SGSI.

j. Preparar uma Declaração de Aplicabilidade."

A política de segurança da informação relaciona-se com a gestão de riscos na sua fase de definição de contexto. Ela deve conter elementos que explicitem o escopo e os limites que serão considerados no SGSI e consequentemente na gestão de riscos.

A figura a seguir indica as etapas do processo de gestão de riscos em segurança da informação. A primeira etapa desse processo é definição do contexto, e nessa etapa é que a política de segurança da informação se faz presente, registrando e explicitando o que deverá ser considerado para o contexto da gestão de risco.

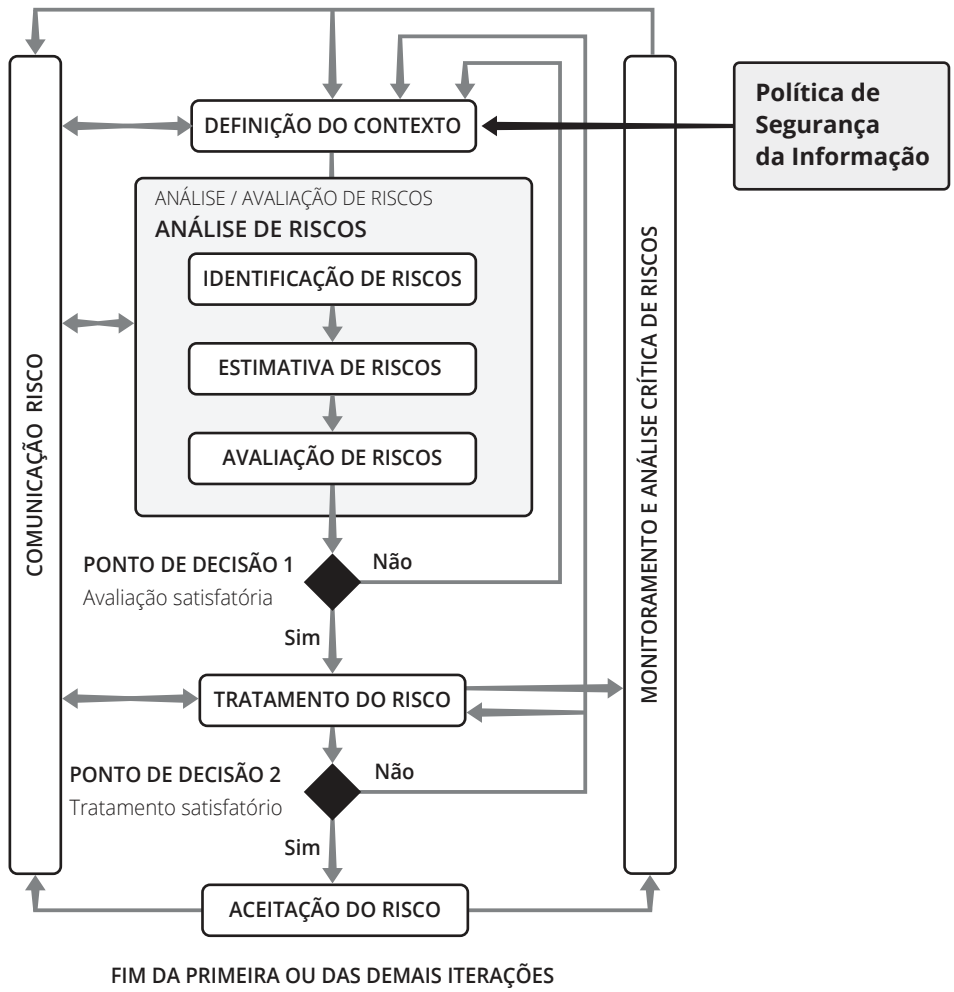


Figura 1.3
Processo de gestão de risco de segurança da informação.

A figura a seguir apresenta as etapas do Modelo PDCA e o seu relacionamento com as etapas de um Processo de Gestão de Riscos de Segurança da Informação.

Processos do SGSI	Processo de gestão de riscos de SI
Planejar	▫ Definição do contexto ▫ Análise / avaliação e riscos ▫ Definição do plano de tratamento de riscos ▫ Aceitação do risco
Executar	▫ Implementação do plano de tratamento de risco
Verificar	▫ Monitoramento contínuo e análise crítica de riscos
Agir	▫ Manter e melhorar o processo de gestão de risos de segurança da informação

Tabela 1.1
Relacionamento dos processos do SGSI e dos processos de gestão de riscos de TI.

Essa norma estabelece que os critérios pelos quais os riscos serão avaliados deverão ser estabelecidos pela política do SGSI. A NBR ISO/IEC 27001:2006, nos itens 4.2.1.b.4 e 4.2.1.c.2, indica que a política do SGSI deve "estabelecer critérios em relação aos quais os riscos serão avaliados" e precisa "desenvolver critérios para que a aceitação de riscos e identifique os níveis aceitáveis de riscos" (ABNT, 2006, página 4-5).

A Política do SGSI possibilita a análise ou avaliação dos riscos e define os elementos para possibilitar o tratamento dos riscos. A Dimensão Política de Segurança da Informação possibilita a Dimensão Gestão de Riscos.

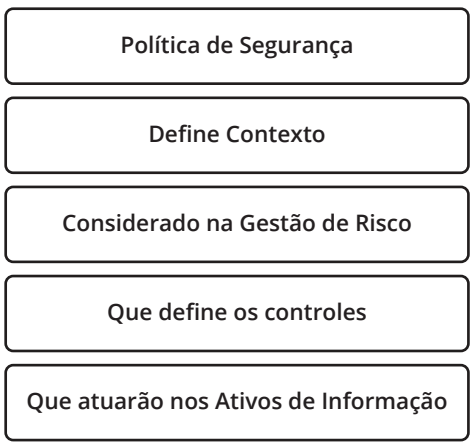


Figura 1.4
Política de Segurança e o Contexto da Gestão de Risco.

Política de segurança da informação e a governança da segurança da informação

O IBGC (2009, página 19), em seu *Código de Melhores Práticas de Governança Corporativa*, define Governança Corporativa como:

"Sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgão de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade."

São quatro os princípios básicos da Governança Corporativa (IBGC, 2009):

- **Transparência**: prover informações relevantes, não apenas as obrigatórias por lei, de forma clara e tempestiva a qualquer interessado;
- **Equidade**: tratamento, de forma justa, de todos os stakeholders, bem como não adoção de práticas ou políticas discriminatórias;

- **Prestação de Contas**: prestação de contas de todos os sócios, conselheiros fiscais e auditores (agentes de governança), dos seus atos administrativos, assumindo toda e qualquer consequência pelos seus atos;
- **Responsabilidade corporativa**: os agentes de Governança Corporativa devem tomar decisões visando à continuidade do negócio, de forma ética, sem se esquecerem da sociedade e do meio ambiente.

Para atender a esses princípios, a organização precisa de informação confiável. Por causa dessa necessidade, a informação tornou-se um recurso crítico. Essa criticidade é explícita pelo ITGI (2006, página 7):

"Informação e sistemas que tratam esta informação são críticos para a operação de todas as organizações. O acesso confiável à informação se tornou um componente indispensável na condução do negócio; além do que, para um crescente número de organizações, informação é o negócio.

Esta crescente dependência pela informação foi identificada há cerca de uma década, quando Peter Drucker afirmou que "a difusão da tecnologia e a mercantilização da informação transformou o papel da informação em um recurso de igual importância à terra, trabalho e capital.'"

Com a implantação da Governança Corporativa, a segurança da informação deixou de ser um controle específico da Área de Tecnologia da Informação para ser um elemento do negócio e da gestão desse negócio.

Nesse sentido, a alta direção e os executivos devem (ITGI, 2006, página 9):

- Entender a criticidade da informação e da segurança da informação na organização;
- Rever o investimento da segurança da informação considerando o alinhamento da segurança da informação com a estratégia de negócio da organização e com o perfil de risco definido pela organização;
- Dar efetivo apoio ao desenvolvimento e implantação de um abrangente programa de segurança da informação;
- Exigir relatórios periódicos da gerência sobre o desenvolvimento e efetividade dos requisitos definidos pela alta direção.

Também devem considerar a (ITGI, 2006, página 9):

- Crescente dependência em relação à informação, aos sistemas e aos recursos de comunicação que possibilitam o uso da informação na organização;
- Dependência de outras entidades;
- Crescente demanda de compartilhar informações com parceiros, fornecedores e clientes;
- Impacto na reputação e no valor da companhia em função de falhas na segurança da informação;
- Falha na dosagem da importância da segurança da informação para a alta direção.

Cresce a necessidade de uma orientação vinda da alta administração com diretrizes de como a organização deseja tratar a informação e a proteção da informação. Para isso, é necessária uma Governança de Segurança da Informação.

O ITGI define a Governança da Segurança da Informação como um subconjunto da Governança Corporativa que fornece orientação estratégica e assegura que os objetivos serão alcançados, gerencia os riscos adequadamente, garante o uso dos recursos organizacionais de maneira responsável e monitora o sucesso ou fracasso do programa corporativo de segurança da informação (ITGI, 2006, página 17).

Para a existência de uma estrutura básica de Governança de Segurança da Informação, o ITGI considera obrigatório (ITGI, 2006, página 18):

- Uma metodologia para gerenciamento de riscos em segurança da informação;
- Uma abrangente estratégia de segurança explicitamente conectada aos objetivos de negócio e aos objetivos de TI;
- Uma estrutura organizacional de segurança da informação eficiente;
- Uma estratégia de segurança da informação que explicite o valor da informação protegida e informação entregue;
- *Políticas de segurança da informação que direcionem cada aspecto da estratégia e dos requisitos definidos em regulamentação* (grifo nosso);
- Um completo conjunto de padrões de segurança para cada política definida, de maneira a garantir que os procedimentos e diretrizes estão coerentes com a política;
- Um processo de monitoramento institucionalizado para garantir o cumprimento e dar o retorno sobre a eficácia da minimização do risco;
- Um processo para assegurar uma avaliação contínua e atualizada das políticas de segurança, padrões, procedimentos e riscos.

É evidente que Dimensão de Política de Segurança da Informação é um elemento crítico para a existência da Governança da Segurança da Informação.

A figura a seguir apresenta uma representação conceitual da Governança de Segurança da Informação.

O centro da figura indica uma sequência de prioridades:

- Ter a Estratégia do Negócio (Business Strategy);
- Definir a Estratégia de Segurança da Informação e de Gestão de Risco (Risk Management/Information Security Strategy);
- Desenvolver os Planos de Ação, Políticas e Padrões (Security Action Plans, Policies and Stardards).

O grupo à esquerda indica o nível ou hierarquia dos profissionais envolvidos e o grupo à direita indica os produtos elaborados.

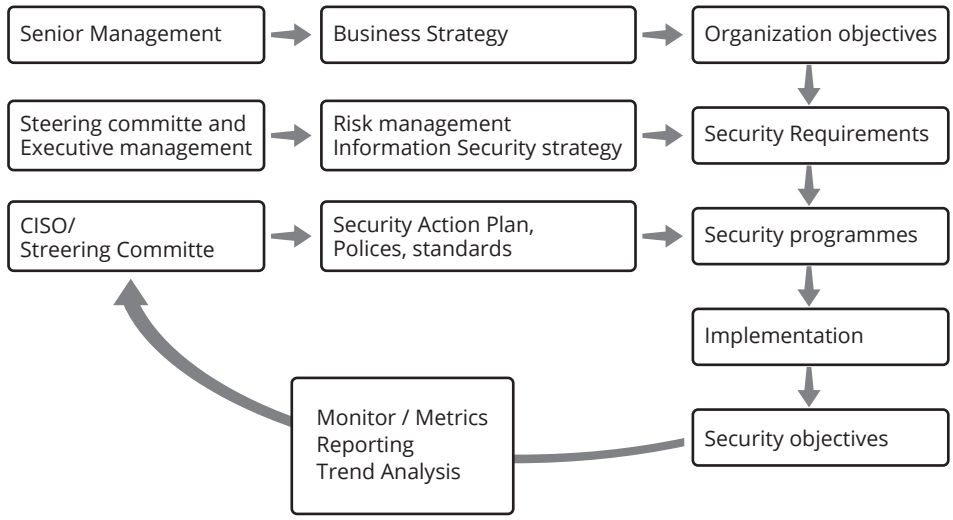


Figura 1.5
Estrutura Conceitual da Governança de Segurança da Informação.

A Norma "NBR ISO/IEC 27014 – Tecnologia da Informação – Técnicas de Segurança – Governança de Segurança da Informação" foi lançada no Brasil no segundo semestre do ano de 2013. Ela fornece uma orientação para a implementação e continuidade da governança de segurança da informação em uma organização.

Definições principais dessa norma:

a. "Governança de segurança da informação

- Governança de segurança da informação é o sistema pelo qual as atividades de segurança da informação de uma organização são dirigidas e controladas (ABNT, 2013, NBR 27014, página 1).

b. Objetivos da governança de segurança da informação:

- Alinhar os objetivos e estratégia da segurança da informação com os objetivos e estratégia do negócio;
- Agregar valor para o corpo diretivo e para as partes interessadas;
- Garantir que os riscos da informação estão sendo adequadamente endereçados (ABNT, 2013, NBR 27014, página 2).

c. Resultados desejados da governança de segurança da informação:

- Visibilidade do corpo diretivo sobre a situação da segurança da informação;
- Uma abordagem ágil para a tomada de decisões sobre os riscos da informação;
- Investimentos eficientes e eficazes em segurança da informação;
- Conformidade com os requisitos externos (legais, regulamentares e contratuais) (ABNT, 2013, NBR, 27014, página 2).

d. Princípios da governança da segurança da informação.

- Estabelecer a segurança da informação em toda a organização;
- Adotar uma abordagem baseada em riscos;
- Estabelecer a direção de decisões de investimento;
- Assegurar conformidade com os requisitos internos e externos;
- Promover um ambiente positivo de segurança;
- Analisar criticamente o desempenho em relação aos resultados de negócios;
- (ABNT, 2013, NBR 27014, página 4 e 5).

e. Responsabilidade pela segurança da informação.

- O corpo diretivo é o maior responsável pelas decisões de uma organização e pelo seu desempenho. Em relação à segurança da informação, o foco principal do corpo diretivo é garantir que a abordagem da organização para a segurança da informação seja eficiente, eficaz, aceitável e alinhada com os objetivos e estratégias de negócios, dando a devida consideração às expectativas das partes interessadas (ABNT, NBR 27014, 2013, página 2).

f. Elementos da direção organizacional

- Corpo diretivo: pessoa ou grupo de pessoas que são responsáveis pelo desempenho e conformidade da organização.
- Gerência executiva: pessoa ou grupo de pessoas que possuem reponsabilidade delegada pelo corpo diretivo para a implementação de estratégias e políticas para alcançar o propósito da organização (ABNT, NBR 27014, 2013, página 1)."

Política de segurança da informação e o Information Technology Infrastructure Library – ITIL

Information Technology Infrastructure Library (ITIL) é uma estrutura que contém um conjunto de diretrizes e práticas recomendadas que visa ajustar pessoas, processos e tecnologia para aumentar a eficiência no gerenciamento de serviços.

O ITIL possui cinco Funções de Serviço:

Service Strategy (Estratégias de Serviços)

Suas funções têm como foco resultados do cliente:

- Composição da Estratégia;
- Gerenciamento Financeiro;
- Gerenciamento Portfólio Serviços;
- Gerenciamento da Demanda.

Service Design (Desenho de Serviços)

Suas funções fornecem orientações sobre a produção e manutenção de políticas de TI, arquiteturas e documentos para o projeto de soluções de TI:

- Gerenciamento Catálogo Serviços;
- Gerenciamento de Nível de Serviço;
- Gerenciamento da Capacidade;
- Gerenciamento da Disponibilidade;
- Gerenciamento da Continuidade;
- *Gerenciamento Segurança Informação* (grifo nosso);
- Gerenciamento de Fornecedores.

Service Transition (Transição de Serviços)

Suas funções fornecem orientações e atividades do processo de transição dos serviços no ambiente de negócios operacionais.

- Planejamento;
- Gerenciamento de Mudanças;
- Gerenciamento da Configuração;
- Gerenciamento da Liberação;
- Validação e Teste;
- Avaliação;
- Gerenciamento Base Conhecimento.

Service Operation (Operação de Serviços)

Suas funções apresentam as atividades de controle para alcançar a excelência operacional no dia a dia.

- Gerenciamento de Eventos;
- Gerenciamento de Incidentes;
- Requisição;
- Gerenciamento de Problemas;
- Gerenciamento de Acessos.

Continual Services Improvment (melhoria contínua de serviços)

Essa função enfatiza a importância da melhoria contínua como parte da qualidade do serviço.

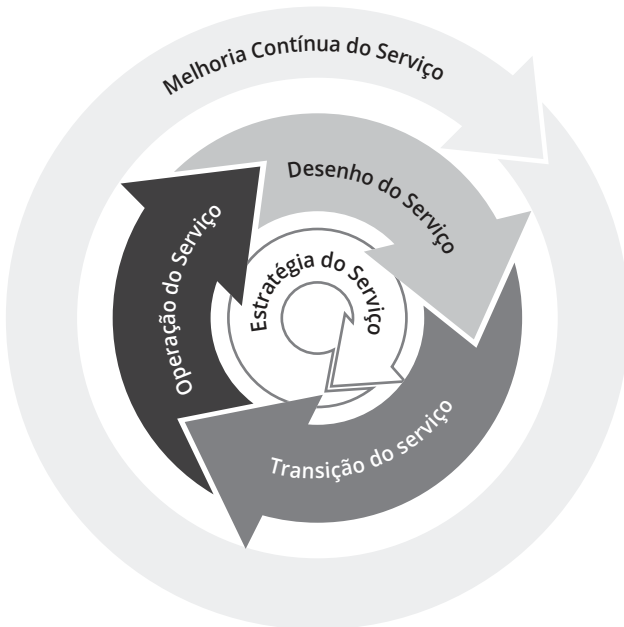


Figura 1.6
Serviços do ITIL.

A figura apresenta os Serviços do ITIL de uma maneira estruturada e como eles devem interagir. Como centro de todas as ações encontram-se as Estratégias do Serviço, garantindo que os demais elementos do ciclo de vida do serviço estarão com foco em resultados do cliente. Ao redor e de uma maneira contínua estão o Desenho de Serviços, a Transição de Serviços e a Operação de Serviços. Esse encadeamento demonstra a continuidade dessa sequência, aprimorando sempre, pois todo esse ambiente está envolvido pela Melhoria Contínua de Serviços.

Na Estrutura ITIL, a Segurança da Informação aparece como uma função do Service Design (Desenho de Serviços).

Segundo a OGC (2007), o objetivo do Gerenciamento de Segurança da Informação é alinhar a segurança de TI com a segurança do negócio e garantir que a segurança da informação está efetivamente gerenciada em todos os serviços e atividades do Gerenciamento de Serviços.

Para o ITIL, o processo do Gerenciamento de Segurança da Informação contempla:

- "*A produção, manutenção, distribuição e melhoria de uma Política de Segurança da Informação e das demais políticas complementares* (grifo nosso);
- A garantia da adequação dos requerimentos de negócio com a Política de Segurança do Negócio;
- Implementação de um conjunto de controles que suportem a Política de Segurança da Informação e gerencie os riscos associados aos acessos aos serviços, informações e sistemas;
- Documentação de todos os controles de segurança, juntos com a operação e manutenção dos controles e dos riscos associados;
- Gerenciamento dos fornecedores e contratados em relação ao acesso aos sistemas e serviços, em paralelo com o Gerenciamento de Fornecedores;
- Gerenciamento de todas as falhas e incidentes de segurança associados aos sistemas e serviços;
- Melhoria proativa nos controles de segurança, gerenciamento de risco de segurança e na redução dos riscos de segurança;
- Integração dos aspectos de segurança com os demais processos de gerenciamento de serviços de TI (OGC, Service Design, página 245)."

O documento do Service Design indica quais políticas relativas à segurança da informação devem existir, OGC (2007):

- Uma política de segurança da informação de mais alto nível;
- Política sobre o uso de recursos de TI;
- Política de controle de acesso;
- Política de uso de e-mail;
- Política de uso de internet;
- Política de uso de antivírus;
- Política de classificação de documento;
- Política de acesso remoto;
- Política de acesso a serviços de TI por fornecedores;
- Política de uso de ativos.

A Dimensão Política de Segurança da Informação é um elemento crítico na Função Gerenciamento da Segurança da Informação. Para uma organização estar alinhada ao ITIL ela precisa desenvolver, implantar e manter a Dimensão Política de Segurança da Informação.

Política de segurança da informação e o Control Objectives for Information and Related Thechnology – COBIT

A Governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e suas estratégias (ITGI, 2007).

O COBIT tem por objetivo definir controles que possibilitarão à área de Tecnologia da Informação cumprir seus objetivos, estando alinhado aos objetivos de negócio.

De acordo com o ITGI (2007), os principais objetivos do COBIT são:

- Estabelecer relacionamentos com os requisitos do negócio;
- Organizar as atividades de TI em um modelo de processo;
- Identificar os principais recursos de TI;
- Definir os objetivos de controle que serão considerados para a gestão.

O COBIT consiste em objetivos de negócios ligados aos objetivos de Tecnologia da Informação, provendo métricas e modelos de maturidade para medir a sua eficácia e identificando as responsabilidades relacionadas aos donos dos processos de negócios e de TI (ITGI, 2007).

Em um dos grupos de controles encontram-se os controles relacionadas à política de segurança da informação. Porém, o próprio COBIT indica que, em relação ao assunto segurança da informação, o usuário pode obter informações detalhadas consultando o padrão ISO 17799, que foi transformado na NBR ISO/IEC 27002 (ITGI, 2007, página 30):

"Todos os usuários em potencial podem se beneficiar da utilização do conteúdo do COBIT como um enfoque geral para o gerenciamento e governança de TI em conjunto com os seguintes padrões mais detalhados:

- ITIL para entrega de serviços;
- CMM para entrega de soluções;
- ISO 17799 para segurança da informação;
- PMBOK ou PRINCE2 para gerenciamento de projetos."

O COBIT considera as atividades de TI em um modelo de processos:

- **PO**: Planejar e Organizar;
- **AI**: Adquirir e Implementar;
- **DS**: Entregar e Suportar;
- **ME**: Monitorar e Avaliar.

No Processo Entregar e Suportar, encontra-se o Processo de TI: Garantir a Segurança de Sistemas.

Domínio Entregar e Suportar – DS – Processos de TI:

- **DS1**: Definir e Gerenciar Níveis de Serviços;
- **DS2**: Gerenciar Serviços Terceirizados;
- **DS3**: Gerenciar o Desempenho e a Capacidade;
- **DS4**: Assegurar a Continuidade dos Serviços;

- **DS5***: Garantir a Segurança dos Sistemas* (grifo nosso);
- **DS6**: Identificar e Alocar Custos;
- **DS7**: Educar e Treinar os Usuários;
- **DS8**: Gerenciar a Central de Serviço e os Incidentes;
- **DS9**: Gerenciar a Configuração;
- **DS10**: Gerenciar Problemas;
- **DS11**: Gerenciar os Dados;
- **DS12**: Gerenciar o Ambiente Físico;
- **DS13**: Gerenciar as Operações.

O escopo desse processo é assim definido (ITGI, 2007, página 119):

"Para manter a integridade da informação e proteger os ativos de TI, é necessário implementar um processo de gestão de segurança.

Esse processo inclui o estabelecimento e a manutenção de papéis, responsabilidades, *políticas* (grifo nosso), padrões e procedimentos de segurança de TI.

A gestão de segurança inclui o monitoramento, o teste periódico e a implementação de ações corretivas das deficiências ou dos incidentes de segurança.

A gestão eficaz de segurança protege todos os ativos de TI e minimiza o impacto sobre os negócios de vulnerabilidades e incidentes de segurança.

"A política de segurança da informação é citada como um dos elementos do Processo de TI Garantir a Segurança dos Sistemas. Ela é indicada no Processo de TI: Plano de Segurança de Tecnologia da Informação, que deve traduzir os requisitos de negócio, de risco e conformidade, em um plano abrangente de segurança de TI, que leve em consideração a infraestrutura de TI e a cultura de segurança."

Esse Plano de Segurança de tecnologia da informação deve ser implementado em políticas e procedimentos de segurança, juntamente com investimentos adequados em serviços, pessoal, software e hardware.

O processo de TI DS5 (garantir a segurança dos sistemas) atende ao requisito de negócio para TI que é manter a integridade da infraestrutura de informação e de processamento, e minimizar o impacto de vulnerabilidades e incidentes de segurança (ITGI, 2007).

A política de segurança da informação está inserida neste processo de TI e está contemplada mais detalhadamente no objetivo de controle DS 5.2 (Plano de Segurança de TI). A Política será considerada em avaliações da Governança de TI que utilizem o COBIT.

Para o COBIT, a Dimensão Política de Segurança da Informação é obrigatória, incrementará o grau de maturidade do processo de tecnologia da informação e suportará melhor o negócio.

2

Arquitetura para a política de segurança da informação

objetivos

Entender a necessidade da existência da política de segurança da informação em uma organização; Conhecer a Arquitetura da Política de Segurança da Informação que define a estrutura do conjunto composto por documentos como Diretriz, Norma e Procedimento; Aprender a definir ações que devem ser realizadas para que a política de segurança da informação seja desenvolvida, validada, aprovada, implantada e mantida, buscando o seu funcionamento adequado na organização.

conceitos

Política de segurança da informação; Arquitetura da Política de Segurança da Informação (diretriz, normas e procedimentos); Desenvolvimento, aprovação e implantação da política de segurança da informação da organização.

Política de segurança da informação

Conforme foi estudado no capítulo anterior, a política de segurança da informação é uma das Dimensões do Processo Organizacional da Segurança da Informação.

A Norma "ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação" indica a necessidade da existência da política de segurança da informação:

"Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes (ABNT, 2013, página 2)."

Peltier (2004) considera a política como o mais alto nível de declaração do que a organização acredita e quer que exista em todas as suas áreas. A política é uma diretiva da direção executiva para criar um programa de segurança da informação, estabelecer seus objetivos e definir responsabilidades. Outros autores colaboram nessa linha de definição:

"Uma política é um guia genérico para a ação. Ela delimita uma ação, mas não especifica o tempo. É uma definição de propósitos de uma empresa e estabelece linhas de orientação e limites para a ação dos indivíduos responsáveis pela implantação. As políticas são princípios que estabelecem regras para a ação e contribuem para o alcance bem-sucedido dos objetivos (Chiavenato, 2010, página 173)."

"Política de segurança é um conjunto de diretrizes gerais destinadas a governar a proteção que será dada aos ativos de informação (Caruso e Steffen, 1999, página 49)."

"Política de segurança é um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações recebam a proteção conveniente que possibilite garantir a sua confidencialidade, integridade e disponibilidade (Barman, 2002, página 4)."

"As políticas são as linhas mestras que indicam os limites ou restrições sobre aquilo que se quer conseguir (Albertin e Pinochet, 2010, página 34)."

O Tribunal de Contas da União apresenta a sua definição de Política de Segurança:

"Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações (Brasil, TCU, 2012, página 10)."

Para o Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional (DSIC) da Presidência da República, conforme descrita em sua Instrução Normativa nº 03 (Diretrizes para a elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal) de 30 de Junho de 2009, a política de segurança da informação "declara o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação e comunicações nos órgãos ou entidades da Administração Pública Federal, direta e indireta".

Porém, a ISO 27002 e as demais normas da família ISO 27000 não definem como deve ser a estrutura do conjunto de documentos que constituirão a política de segurança da informação, bem como de que maneira esses documentos estarão divididos.

O *Manual de Boas Práticas em Segurança da Informação do Tribunal de Contas da União* (Brasil, TCU, 2012) cita alguns tópicos que devem ser considerados na política, mas não define a estrutura dos documentos, apesar de orientar que devem existir vários documentos. Esse manual indica que:

"A Política de Segurança da Informação pode ser composta por várias políticas inter-relacionadas, como a política de senhas, de backup, de contratação e instalação de equipamentos e softwares. Ademais, quando a instituição achar conveniente e necessário que a PSI seja mais abrangente e detalhada, sugere-se a criação de outros documentos que especifiquem práticas e procedimentos e que descrevam com mais detalhes as regras de uso da tecnologia da informação (Brasil, TCU, 2012, página 12)."

Em relação aos elementos que devem compor a política de segurança da informação, o DSIC, na Norma Complementar nº 03, indica que no mínimo devem ser tratados estes assuntos:

- Tratamento da Informação;
- Tratamento de Incidentes de Rede;
- Gestão de Risco;
- Gestão de Continuidade;
- Auditoria e Conformidade;
- Controles de Acesso;
- Uso de e-mail;
- Acesso à internet.

Em relação à necessidade de existência de políticas, no Acórdão (2471/2008-Plenário) o TCU recomendou ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a criação de procedimentos para a elaboração de Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade de Negócio (Brasil, TCU, 2012, página 37).

Em outro Acórdão (1382/2009-Plenário), o TCU recomendou que se defina e implante uma política de segurança da informação para toda a organização, que se estabeleça normas e princípios norteadores da gestão da segurança da informação no Ministério, alinhado aos objetivos de negócio do órgão, conforme orientações contidas na NBR ISO/IEC 27002:2005 e nas orientações dispostas no CobIT 4.1, item DS5.2-Plano de Segurança da TI (Brasil, TCU, 2012, página 44).

Os exemplos citados são Acórdãos que são documentos emitidos pelo TCU e orientados para determinadas instituições. Porém, o exemplo demonstra a exigência de uma política de segurança da informação para as instituições.

Muitas organizações começam a desenvolver seus documentos de política de segurança da informação sem definir ou adotar alguma estrutura e planejamento. O que acontece na prática é um conjunto de documentos confusos, de difícil leitura, com assuntos repetidos ou com falta de assuntos de segurança da informação.

Desta maneira é necessária a utilização de uma Arquitetura para a Política de Segurança da Informação da organização. Essa arquitetura deve definir como os diversos tipos de documentos se relacionarão entre si, como será a hierarquia desses documentos e como os assuntos relacionados à segurança da informação estarão segmentados.

a. Arquitetura para a Política de Segurança da Informação

Para a elaboração de um conjunto de regulamentos (diretriz, normas e procedimentos) é necessária a existência de uma arquitetura que estruture como se relacionarão esses regulamentos.

A arquitetura é a estrutura que permite que a Organização entenda e planeje (antes de ter os regulamentos), como será o seu conjunto de documentos que terão nos seus textos as regras de segurança da informação que deverão ser seguidas por todos. A arquitetura utilizada neste curso foi apresentada em seminários e congressos, aceita por organizações, utilizada como referência na construção e aprimoramento de várias centenas de regulamentos e está formalizada no livro *Políticas e Normas para a Segurança da Informação* (Edison Fontes, Editora Brasport, Rio de Janeiro, 2012, 1ª Edição).

A seguir, são apresentadas as diversas características dessa arquitetura.

Estrutura de níveis de detalhamento dos controles de segurança

Essa arquitetura possui a seguinte estrutura de níveis de detalhamento (granularidade) de controles de segurança da informação.

a. Nível 1 – Documento Diretriz ou Política Principal

Esse documento descreve a filosofia da organização em relação à segurança da informação. Indica os princípios que a organização deseja que sejam seguidos por todos os usuários (funcionários, estagiários, prestadores de serviço, visitantes e outros específicos) da organização e que devem ser a base para os documentos que vão conter as regras mais detalhadas para cada dimensão da segurança da informação. Esse documento, Diretriz ou Política Principal, contém os controles básicos que a organização quer.

Considerando que ele explicita o que se quer, dificilmente os controles definidos nesse documento serão alterados ao longo do tempo. Para tanto, não deverão ser indicadas tecnologias específicas, que estarão rapidamente obsoletas, neste documento.

Esse documento, Diretriz ou Política Principal deve ser assinado pelo representante máximo da organização (presidente, diretor ou reitor) ou deve ser aprovado em reunião com ata formal pela instância administrativa máxima da organização (conselho ou diretoria). Esse segundo caso se torna imprescindível quando, por exemplo, os conselheiros utilizam os sistemas de informação e recebem identificação e autenticação para o acesso à informação em segurança da informação. Esse documento não detalha como serão implantados esses controles. Não indica como nem em que tempo e restrições esses controles acontecerão.

Esse documento, Diretriz ou Política Principal de Segurança da Informação deve ser elaborado de maneira que não necessite ser alterado nos próximos cinco a dez anos.

Exemplo de controle descrito no Documento de Diretriz ou Documento de Política Principal: a identificação de cada usuário da informação é individual e intransferível. A autenticação do usuário é individual e garante a veracidade da identificação.

b. Nível 2 – Documento Norma da Dimensão ou Política da Dimensão

Os documentos que formarão o Nível 2 da Estrutura da política de segurança da informação da organização, definirão, cada um, as regras básicas (controles básicos) para cada Dimensão da Segurança da Informação.

Os controles básicos dos documentos desse Nível 2 devem estar coerentes com os controles estruturais (filosóficos) definidos na Diretriz ou Política Principal e começam a detalhar como os controles devem ser implantados.

Exemplo de controle descrito no Documento Norma da Dimensão ou Política da Dimensão: quando a autenticação for realizada por uso de senha, esta deve ser secreta, de uso e conhecimento exclusivo do usuário. Nem mesmo a chefia pode solicitar a senha de um usuário.

Os controles definidos nessas Normas devem ser detalhados de maneira a indicar como eles devem ser desenvolvidos e implantados. O Nível 2 deve apresentar as regras básicas para a dimensão que está sendo tratada. Casos específicos como controles diferentes que devem ser implementados em cada dimensão devem ser abordados em detalhes nos documentos que serão criados no Nível 3.

É importante que a organização tenha um documento de Nível 2 para cada Dimensão de Segurança da Informação considerada no Processo de Segurança da Informação da organização.

c. Nível 3 – Documento Procedimento de Ação, Documentação ou Orientação Técnica.

Esse documento detalha as ações que devem ser executadas, ou descreve uma documentação, ou descreve um procedimento técnico que deve ser seguido para que os controles definidos na Norma da Dimensão (Política da Dimensão) ou na Diretriz (Política Principal) possam ser desenvolvidos e implantados na organização.

Os documentos elaborados para esse nível e níveis abaixo possuem um grande detalhamento. São esses documentos que vão complementar e permitir que a organização tenha as definições para a operacionalização dos controles e, dessa maneira, desenvolva, implante e mantenha com sucesso a política de segurança da informação, que é a base para o Processo Organizacional da Segurança da Informação.

d. Níveis seguintes

Para efeito formal da arquitetura, os níveis serão definidos até o Nível 3 – Documento Procedimento de Ação, Documentação ou Detalhamento Técnico. Porém, níveis mais detalhados podem e devem ser definidos quando isso for necessário para a sua organização. O entendimento dos três níveis apresentados permite que o leitor e aluno entenda a estrutura e, se necessário, defina níveis mais detalhados de regulamentos de segurança da informação para a sua organização.

e. Visualização da Estrutura da Arquitetura da Política de Segurança da Informação

A figura a seguir representa a estruturação da Arquitetura da Política de Segurança da Informação. No primeiro nível deve existir um documento Diretriz ou Política Principal, no segundo nível devem existir documentos de Norma da Dimensão ou Política da Dimensão e no terceiro nível devem existir documentos que detalhem ações, indiquem padrões técnicos ou registrem documentação.

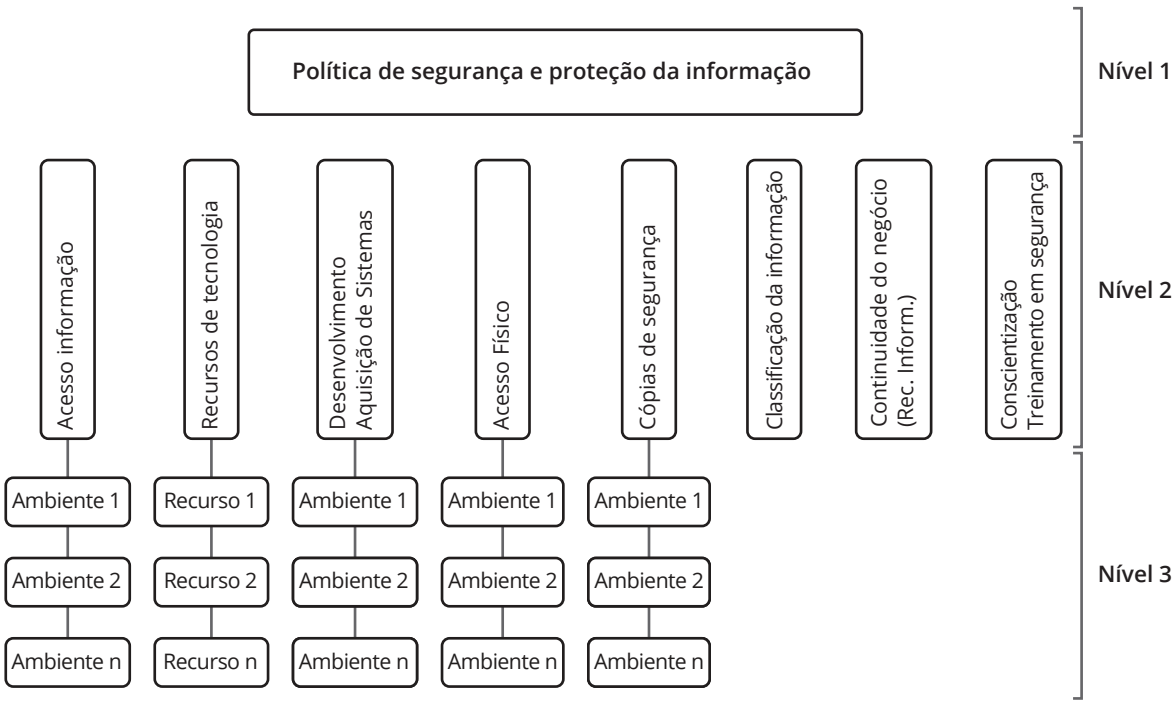


Figura 2.1 Estrutura da Arquitetura da política de segurança da informação.

Elementos da arquitetura da política de segurança da informação

Neste capítulo serão detalhados os elementos e os assuntos que compõem a Arquitetura da Política de Segurança da Informação.

Diretriz ou Política Principal

Esse documento define as regras básicas e os fundamentos para o processo de segurança da informação da organização. Tudo o que for explicitado nesse documento deverá ser descrito com mais detalhes nos documentos dos Níveis 2 e/ou 3, indicando como deverá ser executado.

Exemplo de controle descrito no Documento Procedimento de Ação, Documentação ou Detalhamento Técnico: quando ocorrer esquecimento da senha no ambiente computacional, X o usuário deve seguir os seguintes procedimentos: Segue a lista de procedimentos que o usuário deve fazer quando for solicitar uma nova senha. (...)

Cada uma das dimensões da segurança da informação deve ser considerada nesse documento de maneira que a direção da organização explicite as regras básicas e norteadoras de cada dimensão.

Deve existir apenas um Documento de Diretriz ou Política Principal da Segurança da Informação.

Esse documento deve ser assinado pelo Presidente da organização, ou aprovado pelo Conselho da organização ou aprovado por outro órgão-pessoa que tenha poder hierárquico para garantir que todas as pessoas que lerão o documento entenderão que essas regras são sérias, são para todos os usuários e são mandatórias.

Norma da Dimensão ou Política da Dimensão

a. Acesso Lógico

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao acesso lógico da informação.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. O detalhe de cada ambiente de tecnologia deve ser definido em um documento de acesso lógico de cada ambiente, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

b. Acesso Físico

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao acesso físico que contém recursos de informação.

Devem ser detalhados controles e regras que são comuns a todos os ambientes físicos. Os controles específicos para cada ambiente físico devem ser definidos em um documento de acesso físico de cada ambiente, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

c. Correio eletrônico

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao uso de correio eletrônico pelos usuários.

Devem ser detalhados controles e regras que são comuns a todos os tipos de correio eletrônico utilizado pelos usuários da organização. Controles de segurança da informação específicos para cada tipo de correio eletrônico devem ser definidos em um documento de correio eletrônico – ferramenta específica, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

d. Internet

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao uso do ambiente geral da internet pelos usuários.

Devem ser detalhados controles e regras que são comuns ao ambiente geral da internet utilizado pelos usuários da organização.

e. Redes Sociais

Esse documento detalha os princípios básicos definidos de segurança da informação na Política Principal em relação ao uso de ferramentas de rede social pelos usuários.

Este assunto pode ser englobado na Dimensão Internet, porém por possuir características específicas, recomendamos um documento separado para este assunto, facilitando assim a sua manutenção.

Devem ser detalhados controles e regras que são comuns a todos os tipos de ferramentas de rede social utilizadas pelos usuários da organização. Controles de segurança da informação específicos para cada tipo de ferramentas de rede social devem ser definidos em um documento de rede social – ferramenta específica, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

f. Equipamentos de Tecnologia da Informação

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao uso dos equipamentos de tecnologia da informação pelos usuários.

Devem ser detalhados controles e regras que são comuns a todos os tipos equipamentos de tecnologia da informação utilizados pelos usuários da organização. Controles de segurança da informação específicos para cada tipo equipamento de tecnologia da informação devem ser definidos em um documento de equipamento de tecnologia específico, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

g. Classificação do padrão de sigilo de informação

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao padrão de sigilo da informação, isto é, classificação da informação.

Devem ser detalhados controles e regras que são comuns ao padrão de sigilo da informação utilizado pelos usuários da organização. Isso significa que esse documento deve conter quais são os procedimentos para que seja definido o padrão de sigilo de cada informação e também deve conter os controles que devem ser implantados em relação à informação, após esta ser classificada em relação ao seu padrão de sigilo.

h. Desenvolvimento, implantação e manutenção de sistemas aplicativos

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao desenvolvimento, implantação e manutenção de sistemas aplicativos.

Devem ser detalhados controles e regras que são comuns a todos os tipos de sistemas aplicativos desenvolvidos e implantados para a organização. Controles de segurança da informação específicos para cada tipo de sistema aplicativo devem ser definidos em um documento de Desenvolvimento, implantação e manutenção – Sistema aplicativo específico, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

i. Plano de continuidade de negócio

Esse documento detalha os princípios básicos de segurança da informação, definidos na Política Principal, em relação ao uso de recursos de informação necessários para a continuidade do negócio pela organização, quando da ocorrência de uma situação de indisponibilidade de recursos de informação.

Devem ser detalhados controles e regras que são comuns a todos os tipos de plano de continuidade de negócio utilizado pela organização. Controles de segurança da informação específicos para cada tipo de plano de continuidade de negócio devem ser definidos em um documento de plano de continuidade – situação específica, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

j. Cópias de segurança

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao uso de cópias de segurança pela organização.

Devem ser detalhados controles e regras que são comuns a todos os tipos de cópias de segurança utilizados pelas áreas de negócio da organização. Controles de segurança da informação específicos para cada tipo de cópia de segurança devem ser definidos em um documento de cópia de segurança – sistema específico, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

k. Gestão de riscos

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação à Gestão de Riscos pela organização.

Devem ser detalhados controles e regras que são comuns a todos os tipos de gestão de riscos utilizados pela organização. Controles de segurança da informação específicos para cada tipo de gestão de risco devem ser definidos em um documento de gestão de risco – situação específica, padrão Nível 3 na Arquitetura de Política de Segurança da Informação.

Exercício de fixação
Alinhamento aos objetivos da organização

Um fator crítico de sucesso para a política de segurança da informação é a participação da Direção e das Áreas de Negócio. Considere os controles da Norma NBR ISO/IEC 27002 descritos no Capítulo 1 e identifique dez controles que a fazem referência ou exigência da participação da Direção e/ou de outras áreas da organização. Justifique cada controle identificado.

Exercício de fixação
Arquitetura para a Política Segurança Informação

Considere a Arquitetura para a Política de Segurança da Informação apresentada no curso. Considere a sua organização. Indique quais os documentos (ou assuntos de documentos) existem formalmente como regulamento.

Considere a Arquitetura para a Política de Segurança da Informação apresentada no curso.

Defina a Arquitetura de Política de Segurança da Informação que você entende que a sua organização deveria ter.

Considere na sua organização os ambientes físicos, os ambientes de informação convencional, os ambientes de tecnologia e outros elementos que formam o Ambiente da Informação.

Caso considere alguma restrição, indique essa limitação.

a. Como escrever um texto em um documento da política de segurança da informação

Ao escrever um documento, estamos realizando uma comunicação, estamos enviando um conjunto de informações e desejamos que o receptor entenda perfeitamente o que a organização deseja comunicar neste documento. Como estamos tratando de um regulamento integrante da política de segurança da informação, é preciso ter cuidado e estar atento a alguns pontos que devem ser seguidos para se obter o sucesso desejado. Sendo assim, cada documento da política de segurança da informação deve:

b. Ser de fácil leitura e entendimento

O texto de um documento integrante da política de segurança da informação de uma organização deve ser de fácil entendimento e a sua leitura deve ser fácil. Não é no texto de regulamentos de segurança da informação que devemos colocar palavras de difícil entendimento e sofisticar o texto. Devemos ter um texto profissional, porém com palavras comuns que os usuários entendam no seu dia a dia.

c. Ser aplicável à organização

Esses regulamentos de segurança da informação são elaborados para atender o Processo Organizacional da Segurança da Informação. Sendo assim, ele é um elemento para atender um processo organizacional que tem como maior objetivo possibilitar a organização atingir os seus objetivos no que depender da informação ou dos recursos de informação.

Portanto, se é um elemento organizacional, as regras devem ser desenvolvidas de maneira que a organização, ou melhor, os usuários possam cumprir os controles estabelecidos nesse documento.

O desenvolvimento e implantação de documentos de segurança da informação têm como objetivo principal fazer com que a segurança exista verdadeiramente e que os recursos de informação estejam protegidos.

d. Ser possível de ser cumprido

Não devem existir regras e controles que não possam ser cumpridos na organização. Muitas vezes são definidas regras e controles que necessitarão de recursos adicionais para serem cumpridos pelos usuários.

e. Ser possível de a organização absorver

Além dos usuários entenderem a mensagem e a mensagem poder ser cumprida, é necessário que a organização possa absorver os controles descritos no documento. Isso significa que a organização deve ter um Processo Organizacional de Segurança da Informação para que este ambiente possibilite que os controles estabelecidos tenham existência contínua.

f. Ter um texto positivo

O texto, na medida do possível, deve ser um texto positivo e que não transmita mensagem de negação. Não desejamos que o usuário tenha a impressão de que a segurança da informação é apenas proibitiva. Mas, às vezes, teremos dificuldade nessa comunicação.

g. Ser acessível por todos os usuários da informação

O texto do documento integrante da Política de Segurança deve ser acessível por todos os usuários que acessam a informação da organização. Evidentemente, considerando o público-alvo do documento.

h. Considerar as situações de exceção

O documento deve indicar o que deve ser feito caso o usuário encontre uma situação de exceção, não planejada pelos controles do documento.

i. Possibilitar que pessoas diferentes sigam os mesmos procedimentos

O texto do documento deve possibilitar que pessoas, evidentemente devidamente treinadas, executem as mesmas ações ou reações, em circunstâncias similares. A existência de um documento contendo regras e controles deve acabar com a possibilidade de interpretação diferente por usuário.

j. Definir as regras: não teorizar e não ensinar o assunto segurança

O texto de um documento inserido em uma política de segurança da informação tem como objetivo comunicar regras e explicitar o que pode e o que não pode ser feito pelos usuários. Informações complementares e pequenos esclarecimentos podem ser colocados no texto, porém um documento de regulamento não deve ter no seu corpo um texto ensinando sobre segurança da informação. O local adequado para se ensinar segurança da informação é através de um conjunto de ações de treinamento: palestras presenciais, cursos em tempo real, livros ou material desenvolvido especificamente para o usuário da informação da organização.

As ações de conscientização em segurança da informação são obrigatórias e devem ser feitas paralelamente à implantação dos regulamentos.

k. Conter apenas um macro assunto

O texto do documento deve tratar de apenas um macro assunto de segurança da informação. Não devemos misturar assuntos. Fazendo dessa maneira, o trabalho de comunicação ao usuário certo e as ações de manutenção desse documento serão facilitadas. Nenhum usuário gosta de receber um material para leitura maior do que ele precisa.

Se o documento enviado para o usuário tiver dois assuntos e ele só precisa ser comunicado de um deles, corremos o risco dessa comunicação não ter o sucesso esperado, isto é: o usuário não lerá nem mesmo o assunto que lhe diz respeito. Separando em dois documentos com dois macros assuntos, os usuários que precisem saber de apenas um receberam apenas um documento e saberão que aquele assunto lhe diz respeito. Na questão de manutenção, ter dois documentos para dois macro assuntos facilita o controle e também a definição de quem vai assinar o documento.

Essa separação de macro assuntos não possui uma regra explícita. Na prática, é difícil identificar e separar macro assuntos.

Por exemplo: devemos fazer um documento para cada um dos assuntos: internet, rede social e correio eletrônico? Ou faremos um único documento tratando dos três assuntos? Não existe resposta certa ou errada. Existe a solução mais adequada para a sua organização. E nesse caso você deverá definir (e validar com a sua organização) qual a melhor opção.

Para esse exemplo mencionado, sugere-se a criação de três documentos separados.

l. Não referenciar exatamente os documentos de maior detalhamento

Um documento da política de segurança da informação não deve referenciar exatamente a algum documento de maior nível de detalhamento. A razão dessa recomendação é que documentos menos detalhados deverão ser menos alterados que documentos de maior

granularidade de regras. Sendo assim, se os primeiros referenciarem os segundos, muito provavelmente após certo tempo será necessário alterar o documento mais macro porque o documento com mais detalhes foi quebrado em dois ou teve sua referência alterada. A alteração em documento macro acarreta na coleta de novas assinaturas de aprovação, revisões e outras atividades do processo de aprovação, sendo que na sua essência o documento não teve alteração. Esse esforço pode ser evitado citando apenas que existe um documento mais específico, mas sem incluir detalhes.

m. Ser objetivo e eficaz na comunicação

O principal objetivo de um documento que faz parte da política de segurança da informação de uma organização é comunicar corretamente o que os usuários devem executar. Muitas vezes, a comunicação para determinada regra não é fácil de dizer e tende-se a regulamentar ao redor. Recomenda-se que a comunicação tenha um texto positivo, porém o mais importante é que o usuário entenda a regra. Dessa maneira, uma regra definindo "É proibido acessar a internet durante o horário de expediente do usuário" pode ser mais eficaz do que um texto redigido a partir do permitido.

n. Evitar 'dizer' demais ou 'dizer' menos

Ao escrever qualquer texto, principalmente textos de documentos que compõem a política de segurança da informação, é preciso ser efetivo com o tamanho do texto, isto é, a quantidade de palavras do texto. Não podemos ser tão econômicos que o usuário não entenda a mensagem a ser transmitida, mas também não se pode "falar" demais e de uma maneira cansativa, de forma que o usuário ao final não entenda o que a organização deseja transmitir como regra para o usuário.

Concluindo, podemos afirmar que quanto mais confusa for a política, mais atualização frequente será necessária e mais complicado será o treinamento para os usuários.

Se o texto tiver a possibilidade de ser mal interpretado... será mal interpretado.

Exercício de fixação 
Elaboração de política

Considere o padrão de documentos Nível 1 (Diretriz ou Política Principal) e Nível 2 (Norma da Dimensão ou Política da Dimensão). Elabore um único documento definindo as regras para a seguinte situação:

Utilização, pelas pessoas, de TV e outros equipamentos de tecnologia que possam transmitir os jogos da Copa do Mundo de Futebol.

Considere um dos seguintes ambientes a seguir:

a. Emergência de um hospital.
b. Estúdio de emissora de televisão que não vai transmitir os jogos da Copa do Mundo de Futebol.
c. Seminário de padres.
d. Penitenciária de segurança máxima.
e. Penitenciária comum.

f. Ambiente de concurso público, considerando a empresa que operacionalizará o evento, que coincidentemente será realizado no mesmo horário de uma partida do Brasil durante a Copa do Mundo. A data do concurso não pode ser alterada.

Projeto de elaboração da política de segurança da informação – desenvolvimento, implantação e manutenção

Elaborar os documentos e artefatos que vão compor a política de segurança da informação da organização é um projeto que deve seguir os mesmos passos de qualquer outro projeto da organização. Evidentemente, a Gestão de Projetos deve ser acionada e deve fazer o controle do andamento desse projeto.

Este capítulo complementa os controles da Gestão de Projetos e dessa maneira define alguns aspectos específicos relativos ao desenvolvimento dos regulamentos da política de segurança da informação, que devem ser considerados para que o conjunto de documentos que formam a política de segurança da informação da organização atinja o seu objetivo e consequentemente a organização tenha a proteção adequada para a sua informação.

Inicialização do projeto

Nessa etapa devem ser contemplados os seguintes itens:

a. Descrição, justificativa e objetivo do projeto

Deve-se descrever o que será o projeto, qual a justificativa da existência neste momento do projeto e qual o objetivo do projeto.

Esses elementos devem ser registrados para a documentação do projeto da política de segurança da informação da organização. O projeto pode existir por causa de uma legislação que a organização precisa cumprir, exigência do mercado (organizações clientes), pelo entendimento da direção em ter um diferencial competitivo para a organização ou pela razão básica: para que a organização funcione ao longo do tempo é necessário que suas informações estejam protegidas.

b. Escopo considerado

Na descrição da Arquitetura da Política de Segurança da Informação foram apresentados a estrutura, os tipos de documento e as dimensões que devem ser consideradas pela política, bem como a profundidade (granularidade) das regras dessas dimensões.

A política de segurança da informação da organização deve contemplar todas as dimensões e toda a granularidade das regras. Para alcançar esse objetivo, pode ser necessária a realização de vários projetos, que no final cobrirão todo o escopo.

Dessa maneira, cada projeto relativo à política de segurança da informação de uma organização pode ter um escopo limitado, restrito. É fundamental que todos saibam qual o escopo do projeto que está sendo realizado.

c. Possíveis restrições

Considerando o escopo definido, é necessário identificar quais possíveis restrições poderão impedir ou dificultar o sucesso do projeto de política de segurança da informação da organização.

Por exemplo, considerado a elaboração do Documento de Diretriz, uma possível restrição que impedirá a conclusão dessa diretriz é a indisponibilidade do presidente da organização ou outro executivo com poder de aprovação.

d. Premissas assumidas

Ao iniciar o projeto de política de segurança da informação, considerando o escopo definido, é necessária a explicitação das premissas para o projeto. Premissas são definições, ações e comprometimento que acontecerão no projeto. O projeto foi planejado e estimado considerando que as premissas acontecerão.

Uma premissa simples e necessária é a participação da área de Recursos Humanos e da área Jurídica na revisão dos documentos. Quando desenvolvemos um projeto de desenvolvimento ou alteração da política de segurança da informação, essas duas áreas obrigatoriamente precisam participar do projeto. A área de Recursos Humanos deve participar, pois as regras estabelecidas afetam diretamente as pessoas e a área Jurídica precisa participar das revisões de documentos, pois esses documentos serão a legislação interna da organização e não podem estar contrários à legislação vigente. A Área Jurídica deverá analisar se as regras definidas estão gerando algum passivo para a organização.

e. Definição do produto a ser entregue

Como foi dito anteriormente, a política de segurança da informação é um conjunto estruturado de regulamentos, definidos em vários documentos que consideram as dimensões da segurança da informação, e que definem regras em diferentes padrões de granularidade.

É obrigatório que se explicite para cada projeto relacionado à política de segurança da informação qual será o produto final entregue. Essa explicitação deve ser do tipo: um documento de Diretriz ou Política Principal e dez documentos de Políticas de Dimensão. Nesse caso, está facilmente identificado que serão onze documentos e que não teremos nenhum documento de Procedimento.

Desenvolvimento do projeto

Essa etapa trata de elaborar os documentos que vão compor a política de segurança da informação, considerando o escopo definido. Deve-se considerar:

a. Realização de levantamentos

Nessa etapa deve-se levantar tudo o que a organização tem sobre o assunto política de segurança da informação, considerando o escopo definido para esse projeto.

Políticas e projetos antigos e atuais devem ser estudados para um melhor entendimento de sucessos e fracassos. Tudo isso contribuirá para um melhor entendimento de como a organização está em relação à política de segurança da informação.

Os regulamentos em uso, caso existam, serão de grande contribuição para o desenvolvimento do projeto de política de segurança da informação. Com os documentos atuais pode-se identificar, na fase de entrevistas, se a rigidez e os controles existentes estão adequados, são suficientes ou estão atualizados. Todas essas questões serão material de trabalho para o condutor desse projeto, que normalmente será o Gestor da Segurança da Informação.

Evidentemente alguns desses controles devem existir por causa de uma legislação existente, mas mesmo nesses casos o executivo-gestor deve conhecer a legislação e indicar que precisa de um controle que a atenda.

b. Elaboração e realização de entrevistas

A realização de entrevistas, previamente elaboradas, tem como objetivo identificar como a organização deverá definir e construir os controles que estão presentes na política de segurança da informação.

O profissional que estiver conduzindo esse projeto de elaboração da política de segurança da informação da organização precisa retirar e identificar dos executivos dessa organização qual deve ser o padrão de rigidez dos controles de segurança da informação.

O Gestor da Segurança da Informação, ao levar adiante um projeto de construção da política de segurança da informação, deve questionar à organização, perguntando aos seus executivos-gestores qual a rigidez em segurança da informação que a organização deseja ter. O Gestor de Segurança da Informação tem a obrigação de conhecer os controles recomendados nas normas internacionais, nas estruturas aceitas no mercado (COBIT, ITIL e Risco Operacional) e aplicar esses controles na organização. Porém, é responsabilidade dos executivos-gestores indicar o grau de rigidez desses controles.

É usando a entrevista individual ou em grupo que o Gestor da Segurança da Informação conhecerá o que a organização deseja para a segurança da informação e transformar esse conhecimento em textos que formarão os documentos que serão posteriormente discutidos e aprovados pelos executivos-gestores.

c. Elaboração do texto dos documentos

Após o trabalho de identificar o que a organização deseja como segurança da informação, é necessário documentar essa situação.

Essa fase, que pode ser feita em paralelo com a fase anterior, tem por objetivo gerar os documentos que formarão a política de segurança da informação da organização.

Anteriormente foram apresentadas as orientações de como devem ser escritos os textos dos documentos da política de segurança da informação. Nesse capítulo será dada ênfase aos procedimentos para a elaboração e aprovação dos documentos.

É necessária a existência formal de um grupo revisor para cada documento gerado ou para cada tipo de documento.

Mesmo em organizações de grande porte, esse grupo será pequeno, pode-se considerar as pessoas que participaram das entrevistas ou chamar outras que não participaram. Esse grupo deve ser formalmente criado pela direção da organização, pois as tarefas que seus componentes receberão (revisão de texto, revisão da rigidez dos controles e adequação do regulamento à realidade da organização) exigirão tempo e prioridade. Sem essa formalização dificilmente acontecerá o comprometimento dos participantes com o projeto de política de segurança da informação e, consequentemente, ocorrerão atrasos, possíveis até de impossibilitar o término do projeto.

Para os encontros de revisão, é recomendável pelo menos três rodadas de revisão: inicial, alterada e final.

Nessas revisões presenciais ou por correio eletrônico, é importante lembrar sempre de tratar adequadamente os comentários (sugestões) que não foram aceitos. Eles devem ser registrados e receber um esclarecimento sobre o motivo de não ter sido aceito. As pessoas que estão colaborando com a revisão dos textos precisam ser consideradas. É necessário ter a atenção adequada a elas.

> As sugestões delas podem ou não ser aproveitadas, mas é necessário que suas sugestões sejam respondidas.

Após a definição dos grupos de revisão e com a primeira versão dos documentos ou documento (vide definição de escopo e produto a ser entregue), é necessária a revisão pelo Grupo Revisor. Essa revisão pode acontecer em conjunto, desde que antecipadamente os participantes tenham realizado a leitura, ou pode ser individual. Cada uma dessas opções possui suas vantagens e desvantagens. O gestor da Segurança da Informação que deve estar conduzindo esse projeto deve ter sabedoria suficiente para definir como será a melhor maneira de se fazer a revisão dos documentos.

Após a revisão dos textos dos documentos, é necessário coletar a(as) assinatura(s) do documento.

O responsável pela assinatura de cada documento deve ter o cargo hierárquico compatível com o tipo de documento a ser assinado, bem como ter a competência organizacional sobre o assunto. Normalmente, quem assina o documento participa da etapa de revisão como um participante comum do grupo ou como um concentrador das discussões considerando que ele é quem decidirá no final.

Cada documento construído deve estar dentro do padrão que a organização utiliza para os demais documentos. Os elementos de um documento de regulamento de segurança definidos neste curso no capítulo anterior indicam elementos que devem ser considerados, porém não necessariamente cada um deles precisa ser um item explícito. Se o padrão de documento da sua organização não utiliza aquele elemento como um elemento de destaque, não há problema. O que é exigido é que a definição daquele elemento esteja explicitada.

Produto entregue: documentos aprovados

É necessária que seja realizada uma verificação: os produtos entregues estão coerentes com os documentos aprovados? Aquilo que foi prometido precisa ser formalmente entregue.

Devemos acompanhar, verificar e analisar todos os dias o produto a ser entregue e o produto que está sendo gerado. Nesse curso é apresentada uma ordem, porém é possível que as algumas etapas sejam realizadas em paralelo.

Conhecimento, acessibilidade e treinamento para o usuário: produto gerado

Após a conclusão da construção (ou melhoria) de um documento que participa do conjunto da política de segurança da informação, é necessário garantir o conhecimento do usuário sobre aquele documento, permitir que o documento seja acessado, de maneira manual ou utilizando a tecnologia da informação.

Em certos casos, como no início da existência da política de segurança da informação ou quando é realizada uma alteração ou inclusão muito grande em um determinado assunto de proteção da informação, é obrigatória a realização de um treinamento específico sobre o assunto e específico para os diversos tipos de usuários.

Em resumo, o objetivo dessa fase é fazer com que o usuário entenda que tem novas regras que ele obrigatoriamente terá de cumprir.

Essa etapa deve ser planejada no início do projeto, considerando que a sua realização demandará tempo dos usuários em geral.

Manutenção ou atualização do produto gerado

Essa é uma etapa normalmente desprezada. Parece que quando um projeto gera o produto final estabelecido, tudo termina.

Evidentemente termina uma fase importante, mas há outra tão importante quanto essa, que é a garantia de que o documento gerado e implantado continuará atual e quando for necessário será atualizado no menor tempo possível e adequado para a organização.

Outra questão simples, mas onde muitas organizações cometem erro: garantir que o usuário saiba encontrar os documentos que compõem o conjunto da política de segurança da informação.

Exercício de fixação
Projeto de política

Escolha uma situação da sua organização. Faça um projeto para o desenvolvimento ou melhoria para a política de segurança da informação. Considere os elementos:

- **a:** Descrição, justificativa e objetivo do projeto;
- **b:** Escopo Considerado;
- **c:** Possíveis restrições;
- **d:** Premissas assumidas;
- **e**: Definição do Produto a ser entregue;
- **f**: Responsabilidades para a manutenção do produto gerado;
- **g**: Planejamento do treinamento do usuário.

3

Diretriz ou Política Principal, Política-Norma Dimensão Acesso Lógico e Política-Norma Dimensão Ambiente Físico

objetivos

Conhecer a estrutura básica para os documentos que formarão a política de segurança da informação da organização; Ser apresentado ao Documento Diretriz ou Política Principal, com o seu padrão de profundidade de regras, o seu escopo e o que ele deve considerar; Conhecer a Política Dimensão de Acesso Lógico, com o seu padrão de profundidade de regras, o seu escopo e o que ele deve considerar; Aprender sobre a Política Dimensão de Ambiente Físico, com o seu padrão de profundidade de regras, o seu escopo e o que ele deve considerar.

conceitos

Estrutura de Documento; Documento Diretriz ou Política Principal; Política Dimensão Acesso Lógico; Política Dimensão Acesso Físico.

Estrutura dos documentos que compõem a Arquitetura da Política de Segurança da Informação

Todo tipo de documento relacionado à política de segurança da informação deve ter os seguintes elementos:

- **Objetivo**
- **Escopo**
- **Definições**
- **Regras**
- **Responsabilidades**
- **Cumprimento**

Figura 3.1
Elementos de um regulamento de Segurança da Informação

Objetivo

Esse elemento descreve o objetivo do documento, isto é, explicita o que é tratado no documento. Com esse elemento, o leitor saberá antes da leitura total do documento qual o seu conteúdo.

Além de descrever o que é tratado no documento, esse elemento pode com parcimônia indicar o porquê da existência daquele documento ou daquele assunto.

> É necessário tomar cuidado para que essa explicação não se torne uma aula sobre o tema segurança da informação. Explicações mais detalhadas devem ser apresentadas em um treinamento formal.

Outra questão que pode ser citada é a aderência desse documento aos regulamentos aos quais está seguindo, detalhando ou complementando. Essa referência normalmente diz respeito a documentos em nível superior ao documento em questão.

Escopo

Esse elemento delimita a abrangência de validade do regulamento. Essa limitação pode ser em relação:

- Aos tipos de usuários da informação;
- Ao ambiente físico;
- Ao ambiente de tecnologia;
- Ao tempo de validade;
- Em relação a outros aspectos que possam definir uma limitação.

Definições

Esse elemento deve conter a explicação, detalhamento de termos, siglas, abreviaturas, siglas de elementos organizacionais ou palavras que não são de total conhecimento de todos os leitores do regulamento e, dessa maneira, necessitam de uma explicação indicando o que significa.

Termos em língua estrangeira utilizados no texto devem ser traduzidos. Porém, é preciso lembrar que o documento deve considerar o seu público de leitor alvo. Caso o documento seja um documento técnico e a sua leitura for feita por técnicos de Tecnologia da Informação familiarizados com os termos técnicos em inglês, não será necessário fazer a tradução.

Regras

Esse elemento é o cerne do documento. Aqui estão descritos os controles que devem ser cumpridos pelos usuários.

Deve ser comunicado o que deve ser feito, o que é obrigado a ser feito, o que é proibido de se fazer e outros tipos de regras.

Dependendo do nível de granularidade do documento, isto é, dependendo se o documento é uma Política Principal ou uma Norma Técnica, os controles desse elemento serão mais ou menos detalhados.

As orientações descritas nesse elemento podem e devem ser utilizadas periodicamente em mensagens de conscientização do usuário.

Responsabilidades

Elemento que descreve as responsabilidades das pessoas ou áreas em relação a esse documento. São definidas responsabilidades em relação a:

- Gestão da manutenção da segurança;
- Garantia do entendimento e do conhecimento por todas as pessoas que precisam seguir as regras descritas nesse relatório;
- Realizar revisão periódica do documento e promover a sua atualização quando for necessária;
- Dar conhecimento a cada usuário.

Cumprimento

Nesse elemento devem ser descritas as penalidades para o caso de não cumprimento dos controles aqui descritos, bem como demais controles. Indica comportamentos que não serão aceitáveis. Deve considerar o caso de situações de erro ou de exceção e indicar para o usuário o que deve ser feito nessas situações.

Também deve definir quem é responsável pelo monitoramento do cumprimento desse documento.

Esses elementos podem não existir exatamente nessa ordem ou com esses títulos, porém é fundamental que as definições de cada um dos elementos esteja descrita no documento. Muitas vezes a organização possui uma estrutura de documento que a política de segurança da informação deve seguir. O obrigatório é que o leitor da política encontre a descrição desses elementos no documento.

Documento diretriz ou documento da política principal

O Regulamento Diretriz é o documento de mais alta hierarquia na Estrutura da Arquitetura da Política de Segurança da Informação. Ele define a filosofia da organização em relação à proteção da informação e contém os controles básicos e os fundamentos conceituais que direcionarão o Processo Organizacional de Segurança da Informação.

As definições formalizadas nesse documento deverão ser detalhadas nos demais documentos hierarquizados nos patamares inferiores.

Nesse documento as regras dizem o que a organização deseja como padrão e/ou a rigidez em relação aos controles de segurança da informação. Os documentos situados na Estrutura da Arquitetura de Política em níveis de maior detalhe indicam o como vai ser implementado o controle.

Os documentos de maior detalhamento podem ser agrupados por um determinado escopo tipo: ambiente lógico, ambiente físico ou sub assuntos de cada dimensão.

O Regulamento Diretriz deve considerar cada uma das dimensões da segurança da informação, indicando desta maneira como é o direcionamento que a organização deseja para cada dimensão.

Por ser o documento de mais poder em relação aos critérios de segurança da informação que serão adotados pela organização, esse documento deve ser assinado pelo Presidente da organização ou pelo Conselho de Administração, caso os Conselheiros também venham a se tornar usuários da informação dessa organização.

Essa necessidade de assinatura para formalização pelo Presidente da organização ou pelo Conselho deve-se ao fato de que as regras descritas nesse Documento Diretriz, e nos demais documentos subordinados ao Documento Diretriz, deverão ser cumpridos por todos os usuários. Outro motivo dessa exigência de poder na assinatura desse documento é o fato de que regras descritas nesse Documento Diretriz vão gerar projetos que custam recursos e precisam ser priorizados adequadamente. Finalmente, mais um motivo para essa exigência da assinatura do documento é que a segurança que estamos tratando é da informação da organização como um todo. Não é a segurança da informação da Área de Tecnologia ou da Área de Segurança. É a proteção da informação para os objetivos organizacionais, para garantir o funcionamento da organização no que depender da informação e dos recursos de informação.

Esse documento deve estabelecer as diretrizes principais, considerando as características da organização, para os seguintes elementos de segurança da informação:

- **a**: Acesso à informação;
- **b**: Classificação da informação;
- **c**: Continuidade de negócio;
- **d**: Ambiente de tecnologia;
- **e**: Acesso físico à informação;
- **f**: Conscientização e treinamento de usuários;
- **g**: Modelo operativo da segurança da informação;
- **h**: Flexibilidade operacional;
- **i**: Cópias de segurança;
- **j**: Gestão de riscos em segurança da informação;
- **k**: Desenvolvimento e aquisição de sistemas.

No texto do Documento da Política Principal, esses elementos citados podem ser considerados em tópicos específicos ou considerados em conjunto ou de maneira indireta. O importante é que esses elementos de segurança da informação tenham uma diretriz para permitir a existência de regulamentos nos níveis seguinte.

Exemplo prático de diretriz ou política principal

Política de segurança e proteção da informação

1. Objetivo

Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da organização.

As orientações aqui apresentadas são os princípios fundamentais e representam como a organização exige que a informação seja utilizada.

2. Abrangência

Esta política se aplica:

- A todos os usuários (associados, prestadores de serviços e estagiários) que utilizam as informações da organização;
- A todas as organizações que compõem o Grupo ORGANIZAÇÃO.

3. Implantação

A Gerência de Segurança da Informação coordenará as áreas técnicas, áreas de apoio e as áreas de negócio para desenvolvimento e implantação de projetos, procedimentos, ações, instruções e normativos que possibilitem a operacionalização e manutenção desta política.

4. Diretrizes e regras

4.1. **O bem informação**

A informação utilizada pela organização é um bem que tem valor. A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

4.2. **O Gestor da Informação (GI)**

a. Cada informação deverá ter o seu Gestor, que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação.

b. O Gestor da Informação é a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação.

4.3. **Confidencialidade da informação**

a. O Gestor da Informação classificará o nível de confidencialidade e sigilo da informação baseando-se nos critérios estabelecidos na Norma de Classificação da Informação.

b. A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação e pode ter níveis diferentes ao longo da vida dessa informação.

4.4. **Utilização da informação e recursos**

a. A liberação do acesso da informação para os usuários será autorizada pelo Gestor da Informação, que considerará a necessidade de acesso do usuário e o sigilo da informação para a realização dos objetivos da ORGANIZAÇÃO.

b. O acesso da informação deve ser autorizado apenas para os usuários que necessitam desta para o desempenho das suas atividades profissionais para a organização.

c. Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso consciente a ambientes não autorizados será considerada uma falta grave.

d. O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Esse acesso acontece através da identificação e da autenticação do usuário. Os dados para a autenticação do usuário devem ser mantidos em segredo e possuem o mais alto nível de classificação da informação.

e. Os recursos de tecnologia da organização, disponibilizados para os usuários, tem como objetivo a realização de atividades profissionais. A utilização dos recursos da organização, com finalidade pessoal, é permitida, desde que seja em um nível mínimo e que não viole a Política de Segurança e Proteção da Informação e o Código de Conduta e Ética da organização.

4.5. **Proteção da informação**

a. Toda informação da organização deve ser protegida para que não seja alterada, acessada e destruída indevidamente.

b. Os locais onde se encontram os recursos de informação devem ter proteção e controle de acesso físico compatível com o seu nível de criticidade.

4.6. **Continuidade do uso da informação**

a. Toda informação utilizada para o funcionamento da organização deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção equivalente ao local principal. Esta informação deve ser suficiente para a existência de planos de continuidade de negócio.

b. A criação das cópias de segurança deve considerar os aspectos legais, históricos, de auditoria e de recuperação do ambiente.

c. Os recursos tecnológicos, de infraestrutura e os ambientes físicos onde são realizadas as atividades operacionais do negócio da organização devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade de negócio.

d. A definição e implementação das medidas de prevenção e recuperação, para situações de desastre e contingência, devem ser efetuadas de forma permanente e devem contemplar recursos de tecnologia, humanos e de infraestrutura. Elas são de responsabilidade da diretoria gestora dos recursos, contando com o apoio e validação da Gerência de Segurança da Informação.

4.7. **Computação pessoal e móvel**

As informações estruturadas e sistemas da organização somente serão utilizados em recursos da organização. É proibido o uso de equipamentos pessoais para acessar informações estruturadas e sistemas corporativos da organização.

4.8. **Correio Eletrônico**

a. As mensagens do correio eletrônico disponibilizado para os usuários obrigatoriamente devem ser escritas em linguagem profissional e que não comprometa a imagem da organização, não vá de encontro à legislação vigente e nem aos princípios éticos da organização. Cada usuário é responsável pela conta de correio eletrônico que lhe foi disponibilizado pela organização.

b. O conteúdo do correio eletrônico de cada usuário pode ser acessado e monitorado pela organização quando de situações que ponham em risco a sua imagem, seu negócio ou sua lucratividade. O usuário não deve ter expectativa de sigilo da sua conta de correio eletrônico disponibiliza pela organização para seu uso profissional.

4.9. Ambiente de internet

O ambiente de internet deve ser usado para o desempenho das atividades profissionais do usuário para a organização. Sites que não contenham informações que agreguem conhecimento profissional e para o negócio não devem ser acessados. Os acessos realizados nesse ambiente são monitorados pela organização com o objetivo de garantir o cumprimento dessa política.

4.10. **Redes Sociais**

Os usuários obrigatoriamente devem seguir as regras de uso de Serviços de Rede Social descritos na norma específica.

4.11. **Documentação**

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

4.12. **Conclusão**

a. A utilização das informações do ambiente de tecnologia ou do ambiente convencional pelos usuários da organização deve estar de acordo com os documentos institucionais "Código de Conduta", "Política de Privacidade – Dados Pessoais" e "Conduta Ética e Conflito de Interesses". Todos os usuários devem conhecer e entender esses documentos.

b. A segurança e proteção da informação é uma responsabilidade contínua de cada usuário da organização em relação às informações que acessa e gerencia.

c. Todos os usuários devem utilizar a informação da organização, de acordo com as determinações desta Política de Segurança e Proteção da Informação.

d. O não cumprimento desta política e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui falta grave e o usuário está sujeito à penalidades administrativas e/ou contratuais.

e. A Gerência de Segurança da Informação é a área responsável pela existência efetiva do processo de proteção e segurança da informação da organização.

Informações adicionais poderão ser solicitadas diretamente à Gerência de Segurança da Informação ou encaminhadas através do Help Desk.

Exercícios de fixação
Política Principal

O exemplo dado de Política Principal de Segurança da Informação não contém a definição de Ambiente de Tecnologia e Ambiente Convencional. Defina esses dois termos com o objetivo de facilitar o entendimento por parte dos leitores.

O texto a seguir faz parte da Política Principal de Segurança da Informação. Qual a sua opinião para o termo "... desde que seja em um nível mínimo..." Ele é suficiente para os usuários entenderem e cumprirem? Esse texto seria aplicável para a sua organização? Se não, como você redigira esse texto para a sua organização? Justifique a sua resposta.

Os recursos de tecnologia da organização, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais. A utilização dos recursos da organização, com finalidade pessoal, é permitida, desde que seja em um nível mínimo e que não viole a Política de Segurança e Proteção da Informação e o Código de Conduta e Ética da organização.

Releia o item 4.6 – Continuidade de uso da Informação. Você entende que as regras aqui descritas vão gerar projetos? Quais possíveis projetos precisarão ser desenvolvidos e implementados para atender as regras deste item?

Exercício de fixação
Processo de Segurança da Informação

Quais itens ou trechos do documento exemplo de Política Principal que você entende que precisam melhorar? Indique cinco.

Exercício de fixação
Processo Segurança da Informação

Quais itens ou trechos do documento exemplo Política Principal que você entende que estão muito bons e você destacaria? Indique cinco.

Exercício de fixação
Processo Segurança da Informação

Escreva uma Política Principal de Segurança da Informação para a organização na qual você desenvolve suas atividades profissionais.

Ou escreva uma Política Principal de Segurança da Informação para um hospital.

Ou se for possível e sua organização já possuir uma Diretriz de Segurança da Informação, faça uma análise crítica indicando cinco pontos positivos e cinco pontos a melhorar. Compartilhe com seus colegas de classe.

Documento política da dimensão acesso lógico

Esse documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação ao acesso lógico da informação. Nesse documento a organização explicita como deseja (ou obriga) que o acesso à informação aconteça, seja controlado, auditado, gerenciado e exista ao longo do tempo. As diretrizes definidas nesse documento permitirão o desenvolvimento e implantação de controles de segurança da informação e minimizarão os questionamentos sobre o que pode, o que não pode e o que é obrigatório em relação ao acesso lógico à informação.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. O detalhe de cada ambiente lógico de tecnologia deve ser definido em um documento de acesso lógico de cada ambiente, Padrão Nível 3 na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Esse documento deve considerar e definir as regras para os seguintes elementos de segurança da informação:

a. Gestor da Informação

É a pessoa indicada pela direção da organização que tem o poder para autorizar ou negar o acesso de qualquer usuário à informação sob sua responsabilidade.

b. Gestor do Usuário

É a pessoa que tem o poder de validar informações sobre o usuário, no que diz respeito à sua situação perante a organização.

c. Usuário

É a pessoa que acessa informações da organização para executar suas atividades profissionais.

d. Identificação do Usuário

É a maneira como o usuário será identificado para o ambiente de tecnologia da informação da organização.

e. Autenticação do usuário

É a maneira como o usuário será autenticado para o ambiente de tecnologia da informação da organização.

f. Autorização de acesso

É a maneira como acontecerá a autorização do usuário para acessar as informações da organização.

g. Registro de acesso

É a maneira como será realizado o registro dos acessos realizados nas informações.

h. Custodiante de recurso

É a pessoa ou área responsável pelo adequado funcionamento do recurso de informação.

Exemplo prático de política da dimensão acesso lógico

Política da dimensão acesso à informação

1. Objetivo

Definir os requisitos e regras para o acesso à informação no ambiente de tecnologia.

2. Abrangência

Essa norma se aplica a todos os usuários (associados e prestadores de serviços) que utilizam o ambiente de tecnologia da organização.

3. Implementação

A Gerência de Segurança da Informação e as áreas que suportam a tecnologia da informação são responsáveis pela implementação e continuidade dessa norma de segurança.

4. Política de Segurança e Proteção da Informação

(Itens referentes ao Acesso de Informação – Documento já publicado.)

O Gestor da Informação é a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação.

Cada informação deverá ter o seu Gestor, que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação.

O Gestor da Informação classificará o nível de confidencialidade e proteção da informação baseando-se nos critérios pré-definidos pela Gerência de Segurança da Informação.

A liberação da informação para os usuários será autorizada pelo Gestor, que levará em conta a confidencialidade da informação e a necessidade de acesso do usuário.

Toda informação crítica para o funcionamento da organização deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada. O Gestor da Informação é responsável pela definição dessa criticidade.

5. Definições

5.1. **Gestor da Informação**

É o diretor da área responsável pelo uso dos sistemas e serviços de informação (ou parte deles) que possibilitam a realização das atividades de negócio, administrativas e/ou de apoio.

Cada diretor poderá indicar para os sistemas e serviços sob sua responsabilidade outras pessoas para também exercerem a função de Gestor da Informação.

5.2. **Gestor de Usuário**

É a pessoa que garante para a organização que o usuário está exercendo normalmente as suas atividades profissionais na organização.

O Gestor de Usuário para associado é a sua chefia organizacional a partir do nível gerente ou superior.

O Gestor de Usuário para não associado é o gerente (ou pessoa de nível hierárquico superior) responsável pela contratação da prestação de serviço.

6. Responsabilidades

6.1. **Gestor da Informação**

a. Autorizar (ou negar) o acesso do usuário à informação, considerando
   - A real necessidade de acesso pelo usuário;
   - A confidencialidade da informação;
   - O tipo de acesso (leitura, alteração ou remoção) a ser autorizado.

b. Validar e atualizar, pelo menos a cada seis meses, os usuários que possuem acesso à informação.

c. Definir o nível de classificação de confidencialidade da informação.

d. Definir o impacto para a organização caso a informação esteja indisponível para a realização do negócio.

e. Definir o nível de continuidade de negócio referente ao sistema ou serviço sob sua responsabilidade, validando as soluções para situações de desastre e de contingência implementadas pelas áreas de tecnologia.

f. Definir a necessidade de cópias de segurança e validar as soluções implementadas pelas áreas de tecnologia para o sistemas e serviços sob sua responsabilidade.

g. Validar a eventual necessidade de armazenamento de dados pessoais nos sistemas e serviços sob sua responsabilidade, de forma que esteja coerente com a Política de Privacidade – Dados Pessoais.

h. Buscar junto à organização os recursos que permitam a implantação e manutenção do nível de proteção e disponibilidade desejado para os sistemas ou serviços sob a sua responsabilidade, possibilitando realização do negócio.

6.2. **Gestor de Usuário**

a. Garantir que o usuário somente esteja ativo no ambiente de tecnologia caso esse usuário seja um funcionário ou prestador de serviço exercendo normalmente as suas funções profissionais para a organização.

b. Validar e atualizar, pelo menos a cada trinta dias, os usuários tipo prestador de serviço sob sua responsabilidade.

6.3. **Usuário**

a. Solicitar acesso apenas para as informações que vai utilizar nas suas atividades profissionais na organização.

b. Solicitar o corte de acesso à informação, quando suas atividades profissionais na organização não mais exigirem esse acesso.

7. Procedimentos

7.1. **Inclusão do usuário no ambiente computacional**

a. O Gestor do Usuário autoriza a inclusão do usuário no ambiente computacional.

b. A área responsável pelo cadastro de usuário realiza a inclusão do usuário e arquiva a autorização.

7.2. **Exclusão e manutenção do usuário no ambiente computacional**

a. Sempre que acontece um desligamento de associado, a área de recursos humanos comunica à área de tecnologia responsável pelo cadastro de usuários o nome desses associados.

b. O Gestor de Usuário também deve comunicar à área de tecnologia responsável pelo cadastro de usuários o nome dos associados e de prestadores de serviço que estão sob sua responsabilidade e que deixarão a organização.

c. Para cada prestador de serviço, existirá uma data de expiração de contrato. Após essa data, a identificação do usuário deve perder a validade. Essa data de expiração não poderá ser maior do que seis meses.

d. Periodicamente o Gestor de Usuário validará os usuários tipo prestadores de serviço que estão sob sua responsabilidade.

e. A área responsável pelo cadastro do usuário arquiva a comunicação de manutenção ou exclusão.

7.3. **Acesso à informação**

a. O Gestor da Informação autoriza o acesso do usuário à informação.

b. O Gestor da informação valida periodicamente os usuários que possuem acesso à informação sob sua responsabilidade.

c. Quando de mudança de função profissional dentro da organização, o próprio usuário deve solicitar a exclusão de acesso às informações que não precisa mais para o desempenho das suas atividades profissionais.

d. A área responsável pela liberação do acesso à informação realiza a liberação do acesso, arquiva a autorização de acesso ou a comunicação de corte de acesso.

8. Conclusão

Os Gestores de Informação e de Usuário aprovados pela organização estão com os nomes divulgados na norma de segurança "Gestor de Informação e Gestor de Usuário".

Procedimentos poderão ser formalizados para cada um dos ambientes computacionais com o objetivo de descrever mais detalhadamente as regras aqui definidas.

O não cumprimento das regras descritas neste documento que complementam a Política de Segurança e Proteção da Informação constitui falta grave e o usuário está sujeito a penalidades administrativas e/ou contratuais.

Situações não previstas, dúvidas, informações adicionais e sugestões devem ser encaminhadas à Gerência de Segurança da Informação.

Exercício de fixação
Processo de Segurança da Informação

Quais itens ou trechos do documento exemplo de Política Dimensão Acesso Lógico que você entende que precisam melhorar? Indique cinco. Justifique.

Quais itens ou trechos do documento exemplo Política Dimensão Acesso Lógico você entende que estão muito bons e você destacaria? Indique cinco. Justifique.

Documento política da dimensão no ambiente físico

Este documento detalha os princípios básicos de segurança da informação definidos na Política Principal em relação à proteção da informação no ambiente físico ou ambiente convencional. Neste documento a organização explicita como deseja (ou obriga) que a informação seja cuidada e protegida.

Define também como o uso da informação deve ser controlado, auditado, gerenciado e permaneça ao longo do tempo. As diretrizes definidas neste documento permitirão o desenvolvimento e implantação de controles de acesso e uso da informação armazenada no ambiente físico e explicitará o que pode, o que não pode e o que é obrigatório em relação ao acesso à informação no ambiente físico.

Devem ser detalhados controles e regras que são comuns a todos os ambientes físicos que armazenem informação. O detalhe de cada ambiente físico que contém informação deve ser definido em um documento mais detalhado para cada ambiente físico, Padrão Nível 3 na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Este documento deve considerar e definir as regras para os seguintes elementos de segurança da informação:

a. Gestor da Informação

   É a pessoa indicada pela direção da organização que tem o poder para autorizar ou negar o acesso de qualquer usuário à informação sob sua responsabilidade.

b. Gestor do Usuário

   É a pessoa que tem o poder de validar informações sobre o usuário, no que diz respeito à sua situação perante a organização.

c. Usuário

   É a pessoa que acessa informações da organização para executar suas atividades profissionais.

d. Identificação do usuário

   É a maneira como o usuário será identificado para o ambiente de tecnologia da informação da organização.

e. Autenticação do usuário

É a maneira como o usuário será autenticado para o ambiente de tecnologia da informação da organização.

f. Autorização de acesso

É a maneira como acontecerá a autorização do usuário para acessar as informações da organização.

g. Registro de acesso

É a maneira como a será realizado o registro dos acessos realizados nas informações.

h. Custodiante de recurso

É a pessoa ou área responsável pelo adequado funcionamento do recurso de informação.

Exemplo prático de política da dimensão no ambiente físico

Acesso à informação no ambiente físico (convencional)

1. Objetivo

Definir as regras para o uso da informação no ambiente convencional da organização.

2. Abrangência

a. Aplica-se a toda a informação existente no ambiente convencional da organização.

b. Aplica-se para todo usuário da informação da organização.

3. Referências a outros regulamentos

a. Este documento está alinhado com a Política de Segurança da Informação da organização.

b. Os conceitos e termos definidos na Política de Segurança da Informação são utilizados neste documento.

4. Principais diretrizes

4.1. **Gestor da Informação**

a. Toda informação convencional da organização deve ter o seu Gestor da Informação.

b. O acesso à informação será formalmente autorizado pelo Gestor da Informação que considerará a real necessidade do uso da informação, as atividades do usuário em relação à organização, as possibilidades contratuais de acesso do usuário e o nível de classificação da informação.

c. Tem a responsabilidade de analisar e avaliar as ameaças e os riscos para a liberação do acesso aos recursos físicos que contêm a informação.

d. É o responsável pela definição da necessidade de implantação de controles para o acesso aos recursos físicos que contêm a informação.

4.2. **Gestor de Usuário**

Cada usuário tem definido o seu Gestor de Usuário:

- **Empregado e Estagiário**: Gestor a partir do nível de Supervisor;
- **Demais usuários**: Gestor de Contrato;
- **Outros não considerados**: será definido pelo Departamento de Segurança da Informação.

4.3. **Custodiante do Recurso**

a. Tem a responsabilidade pela integridade, disponibilidade para uso e continuidade do recurso que contêm a informação.

b. É responsável pelo recurso físico que suporta a informação.

c. Deve definir, em conjunto com o gestor da informação, controles para que apenas pessoas autorizadas tenham acesso ao recurso físico que suporta a informação.

d. É responsável por garantir as boas condições e a proteção do ambiente físico onde estão os recursos que contêm a informação.

e. Todo recurso de informação da organização deve ter o seu Custodiante de Recurso.

4.4. **Identificação do usuário**

A identificação de usuário no ambiente convencional será realizada através de crachá funcional ou algum documento legal de identificação que contenha foto do usuário.

4.5. **Autenticação do usuário**

A autenticação do usuário será feita pelo Custodiante do Recurso ou seu representante previamente autorizado e verificará a correta correspondência da pessoa com o documento de identificação apresentado.

4.6. **Acesso à informação**

4.6.1. Solicitação de Acesso à informação

a. Quando se tratar de funcionário da organização, o usuário ou o seu Gestor de Usuário solicita para o Gestor da Informação o acesso à informação.

b. Quando se tratar de não funcionário da organização, o Gestor de Usuário solicita para o Gestor da Informação o acesso à informação.

c. Caso o Gestor da Informação autorize o usuário, este Gestor deve comunicar ao Custodiante do Recurso que contém a informação a autorização de acesso e os referidos limites de acesso.

d. O Gestor da Informação deve definir e indicar para o Custodiante de Recurso o tipo de acesso que o usuário poderá ter ao recurso físico que contém a informação: leitura, retirada ou devolução, cópia, inclusão e/ou destruição.

e. O Custodiante de Recurso após receber a autorização do Gestor da Informação realiza a autenticação do usuário e, sendo uma autenticação válida, permite que o usuário acesse o recurso que contém a informação considerando o tipo de acesso autorizado pelo Gestor da Informação.

4.6.2. Registro de acesso

O Custodiante do Recurso definirá em conjunto com o Gestor da Informação, considerando a necessidade de controles da organização ou a existência de obrigações legais, a necessidade de registro dos acessos realizados aos recursos que contêm a informação, bem como à própria informação. Também deve ser definido o tempo de guarda desse registro de acesso.

4.6.3. Controle sobre o acesso à informação

O Custodiante de Recurso deve manter uma lista com o nome das pessoas que estão autorizadas a acessarem os recursos sob sua responsabilidade.

A cada período de seis meses o Custodiante de Recurso comunica ao Gestor da Informação e aos Gestores de Usuários o nome dos usuários que estão autorizados a acessarem os recursos que contêm a informação. O Gestor da Informação e os respectivos Gestores de Usuários indicam a permanência ou não dos usuários no acesso aos recursos que contêm a informação.

Quando o usuário encerrar suas atividades com a organização, o Gestor de Usuário comunicará esse fato ao Custodiante a quem ele solicitou acesso de usuário.

5. Atribuições e competências

Usuário

Ter a responsabilidade pelo uso e manuseio que fizer na informação que tiver acesso.

Usuário, Gestor da Informação e Custodiante

Conhecer e entender a legislação vigente referente à informação e aos recursos físicos que contêm a informação sob sua responsabilidade.

4

Política-Norma Dimensão Correio Eletrônico, Política-Norma Dimensão Internet e Política-Norma Equipamentos Tecnologia Informação

objetivos

Conhecer os componentes que devem ser considerados em uma Política-Norma Dimensão do Correio Eletrônico; Ser apresentado aos componentes que devem ser considerados em uma Política-Norma Dimensão do Uso da Internet; Saber que componentes que devem ser considerados em uma Política-Norma Dimensão do Uso de Equipamentos de Tecnologia da informação.

conceitos

Política-Norma Dimensão Correio Eletrônico; Política-Norma Dimensão Internet; Política-Norma Equipamentos de Tecnologia da Informação.

Introdução

Os regulamentos apresentados nesta aula estão muito ligados ao seu uso no ambiente corporativo e no seu ambiente pessoal. Normalmente os usuários utilizam correio eletrônico, internet e redes sociais no Ambiente Digital tanto em uma atividade corporativa como em uma atividade pessoal.

Em outras dimensões dificilmente o usuário terá esse forte relacionamento. Por exemplo, na Dimensão de Manutenção de Desenvolvimento de Sistemas dificilmente um usuário terá uma atividade pessoal que requer o desenvolvimento ou manutenção de sistemas aplicativos. Evidentemente, com exceção se o usuário for um profissional de desenvolvimento e manutenção de sistemas.

Sendo assim, este bloco de Políticas-Normas tratam de assuntos que, mais do que nunca, dependem de como a organização quer se relacionar com esses ambientes e qual o grau de rigidez de controle de segurança da informação a organização deseja impor em cada um desses assuntos. Isso significa que podemos ter diferentes estratégias para o tratamento desses aspectos. Uma organização pode bloquear o acesso à internet para todos os usuários, enquanto outra deixa acesso livre para todos os usuários.

O importante é que, para esses dois casos, o Gestor da Segurança da Informação tenha envolvido para a definição dos controles a área de Recursos Humanos e a área Jurídica.

Os aspectos contemplados neste bloco dependem fortemente da cultura da organização e consequentemente das pessoas. A cultura organizacional é um elemento que influencia o Processo Organizacional da Segurança da Informação, mas é fundamental e é obrigatório para o sucesso desse processo que existam formalmente e de maneira estruturada os regulamentos de segurança da informação.

Diversas situações para implementação de determinados controles podem existir de acordo com a natureza da organização. É importante que o Gestor de Segurança da Informação saiba conduzir a discussão na sua organização, para determinar como será o conteúdo dos Documentos Política-Normas das Dimensões aqui consideradas.

Até o ano de 2013 não existia no Brasil uma legislação sobre algumas questões relacionadas fortemente com os elementos deste assunto. O mais comumente encontrado é a jurisprudência sobre diversos assuntos relacionados ao tema Segurança da Informação.

Documento política-norma de correio eletrônico

O Documento Política-Norma de Correio Eletrônico define os princípios básicos de segurança da informação definidos na Política Principal em relação ao uso de Correio Eletrônico na organização.

Quando orientações básicas forem definidas neste documento, elas permitirão o desenvolvimento e a implantação de controles de segurança da informação e minimizarão os questionamentos sobre o que pode, o que não pode e o que é obrigatório em relação ao uso do correio eletrônico pelo usuário.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. Caso existam serviços de Correio Eletrônico em ambientes diferentes e que necessitem de controles específicos, deverão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Este regulamento sobre Correio Eletrônico deve considerar e definir as regras para os seguintes elementos:

a. **Usuários**

Deve-se indicar os tipos de usuários que podem utilizar o serviço de correio eletrônico usando parcialmente ou totalmente recursos da organização.

Deve-se indicar as responsabilidades dos usuários em relação ao uso do correio eletrônico.

b. **Correio corporativo e correio pessoal**

Deve-se considerar o uso do correio eletrônico corporativo e o correio eletrônico pessoal utilizando recursos da organização.

Em relação ao correio eletrônico pessoal, deve-se indicar as restrições e obrigações para o seu uso.

Em relação ao correio eletrônico corporativo, deve-se indicar as regras de controle de segurança da informação e deve-se deixar claro e formalmente entendido pelo usuário que este não deve ter expectativa de privacidade: seu conteúdo e acesso serão monitorados.

Isso significa que achando a organização necessário, será feito uma abertura dos dados do correio corporativo de um usuário.

c. **Linguagem utilizada**

Deve-se orientar o usuário em relação ao tipo de texto utilizado: se mais formal, se menos informal.

d. **Operacionalização**

Deve-se orientar sobre os procedimentos operacionais relativos à segurança, incluindo situações de erro e situações não previstas.

e. **Arquivos anexos**

Deve-se definir (considerando aspectos de segurança) o uso de arquivos anexos. Deve-se lembrar de que esses controles devem estar ligados com outros controles como, por exemplo: classificação da informação.

Exemplo prático de Política-Norma da Dimensão Correio Eletrônico

Uso de correio eletrônico

1. Objetivo

Definir os requisitos e regras de segurança para o uso do correio eletrônico (e-mail) no âmbito da organização.

2. Abrangência

Esta política se aplica a todos os usuários (associados e prestadores de serviços) que utilizam as informações da organização.

3. Implementação

A Gerência de Segurança da Informação e a Área de Apoio ao Usuário Final são responsáveis pela implementação e continuidade desta norma de segurança.

4. Política de segurança e proteção da informação

(Itens referentes ao correio eletrônico – Documento já publicado.)

O correio eletrônico é um instrumento de comunicação interna e externa para a realização do negócio da organização.

As mensagens do correio eletrônico devem ser escritas em linguagem profissional e que não comprometa a imagem da organização, não vá de encontro à legislação vigente e nem aos princípios éticos da organização.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

O conteúdo do correio eletrônico de cada usuário pode ser acessado pela organização quando de situações que ponham em risco a sua imagem e o seu negócio. Esse acesso será feito a critério da organização, mediante comunicação ao superior imediato do usuário, à Gerência de Segurança e deve ser registrado formalmente permitindo uma auditoria desse procedimento.

5. Regras

É obrigatório o usuário cadastrado e autorizado no ambiente de correio eletrônico da organização seguir as seguintes regras:

Uso de mensagens

O usuário:

5.1. Pode enviar mensagens relativas aos negócios da empresa para usuários internos ou para pessoas ou organizações em endereços externos.

5.2. Pode utilizar o correio eletrônico para propósitos pessoais incidentais, desde que sejam em um nível mínimo, não prejudiquem o desempenho dos recursos da organização, não interfiram no desempenho das suas atividades profissionais e não violem a Política de Segurança e Proteção da Informação e o Código de Conduta e Ética da organização.

5.3. Não pode originar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade ou deficiência física;
- Possua informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Possam trazer prejuízo a outras pessoas;
- Sejam hostis ou inúteis;
- Que defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da organização ou seus produtos e serviços;
- Possam prejudicar a imagem de outras companhias;
- Sejam incoerentes com as políticas e códigos da organização.

5.4. Não pode reproduzir qualquer material recebido pelo correio eletrônico ou outro meio que possa infringir direitos autorais, marcas, licença de software ou patentes existentes, sem que haja permissão por escrito do criador do trabalho.

5.5. Nunca deve enviar por correio eletrônico qualquer comunicação que possa ser de alguma maneira incorreta ou não apropriada para envio pelo correio regular em papel timbrado da empresa. Uma mensagem eletrônica é considerada um documento formal da empresa.

5.6. Não pode encaminhar mensagens que representem a opinião pessoal do autor, colocando-a em nome da organização.

5.7. Não pode utilizar o endereço do correio eletrônico da organização para outras atividades profissionais não relacionadas à organização.

5.8. Caso receba uma mensagem originada da internet de um remetente desconhecido, você deve remover essa mensagem da sua caixa de entrada, preferencialmente antes mesmo de abri-la.

5.9. Não deve responder caso receba mensagens contendo texto ou imagem não profissional ou de propaganda. Nem mesmo que seja para solicitar seu não envio. Nesse caso, o remetente saberá que o endereço eletrônico está válido.

Confidencialidade e validade da mensagem

5.10. Enquanto o correio eletrônico não utilizar a Certificação Digital ou qualquer outro processo que garanta a confidencialidade da mensagem e a autenticidade do destinatário ou remetente, você não deve enviar mensagens para fora do domínio organização.com.br em que:

- O destinatário ou a organização ficariam incomodados ou embaraçados se a mensagem fosse publicada na primeira página de jornal de grande circulação;
- Um parceiro (cliente ou fornecedor) autorize determinada ação para a organização e que, futuramente, essa mensagem não seja reconhecida por esse parceiro, trazendo prejuízo para a organização. Para esses casos, o envio de mensagem pode agilizar um processo, porém deve ser formalizado através de um outro meio que confirme a ação solicitada. Para os casos em que uma negociação tenha de ser feita via correio eletrônico, o diretor da área deverá estar formalmente ciente desse fato e do potencial risco para a organização.

5.11. Quando envia uma mensagem de correio eletrônico, ela está restrita a você e ao destinatário. Porém, no caso de informações que exijam maior sigilo, você deve na primeira linha da mensagem indicar o nível de classificação dessa informação, entre os níveis de confidencialidade descritos na Norma de Segurança – Classificação da Informação.

5.12. Caso receba, por algum motivo, uma mensagem que por erro lhe foi enviada, deve proceder da seguinte maneira:

- Caso seja uma mensagem de endereço organização.com.br, informe ao remetente o ocorrido e remova a mensagem da sua caixa de entrada;
- Caso não seja do ambiente organização.com.br, simplesmente remova a mensagem da sua caixa de entrada.

5.13. Ao enviar uma mensagem para um destinatário com cópia para várias pessoas, tenha certeza de que todas essas pessoas realmente devem receber essa mensagem. A facilidade de se copiar uma mensagem no correio eletrônico nos leva a endereçar cópias para muitas pessoas. O mesmo vale para quando vamos responder uma mensagem. Cópias desnecessárias sobrecarregam os recursos do ambiente computacional.

5.14. Ao indicar o destinatário ou o "com cópia", tenha absoluta certeza de que o nome colocado é o nome do usuário para quem você deseja enviar a mensagem. Quando for enviar para vários usuários com certa frequência, utilize a opção de grupo de endereços evitando erros de endereçamento.

5.15. Tenha muita atenção com o uso da opção "Encaminhar/Forward", que vai criando um histórico com todas as mensagens encadeadas. Avalie se é necessário e conveniente o envio de todas essas mensagens. Existe o risco de quebra de confidencialidade da informação e a ocorrência de situações desagradáveis com a leitura indevida de mensagens do correio eletrônico.

Arquivos anexos

5.16. Somente deve enviar arquivos anexados quando for imprescindível. Cuidado quando estiver repassando (Encaminhar/Forward) mensagens para não estar também repassando desnecessariamente arquivos anexados.

5.17. Deve garantir que cada um dos arquivos anexados possuam o seu nível de confidencialidade da informação de acordo com a Norma de Segurança – Classificação da Informação.

5.18. Não deve abrir arquivos anexados de remetentes desconhecidos. Remova esses arquivos do seu ambiente de correio eletrônico.

Gestão do Correio Eletrônico

5.19. Verificar regularmente a sua caixa de entrada do ambiente de correio eletrônico.

5.20. Caso necessite manter a mensagem, verifique seu espaço no servidor de correio eletrônico. Caso esteja perto do limite, transfira esta para uma de suas pastas pessoais. Porém, nesse caso você está sem a facilidade de cópias de segurança que são executadas no servidor.

5.21. Caso necessite de cópias de segurança para suas pastas pessoais, entre em contato com o Help Desk para receber a devida orientação.

5.22. Não compartilhe a sua senha de acesso ao ambiente de rede e ao correio eletrônico com nenhum outro usuário. Caso você necessite que algum outro usuário (por exemplo, uma secretária) tenha acesso ao seu correio eletrônico, faça através dos procedimentos de acesso compartilhado, porém cada usuário deve utilizar sua própria identificação e senha.

5.23. Quando for passar um período sem acessar o correio eletrônico, deixe uma mensagem de ausência e indique quem pode ser procurado no seu lugar.

5.24. Deve cuidar do espaço limitado que cada usuário possui no servidor para sua caixa de entrada, caixa de saída e alguns outros recursos. Quando esse espaço for ultrapassado, haverá restrições para envio e recebimento de mensagens.

6. Conclusão

O não cumprimento das regras descritas neste documento que complementam a Política de Segurança e Proteção da Informação constitui falta grave e o usuário está sujeito à penalidades administrativas e/ou contratuais.

Situações não previstas e sugestões devem ser encaminhada à Gerência de Segurança da Informação.

Dúvidas e informações adicionais poderão ser encaminhadas diretamente ao Help Desk.

Exercício de fixação
Correio eletrônico

No exemplo Política-Norma de Correio Eletrônico temos o seguinte texto:

5.2. Pode utilizar o correio eletrônico para propósitos pessoais incidentais, desde que sejam em um nível mínimo, não prejudiquem o desempenho dos recursos da organização, não interfiram no desempenho das suas atividades profissionais e não violem a Política de Segurança e Proteção da Informação e o Código de Conduta e Ética da organização.

Este trecho de texto está adequado para uso na sua organização? Se não, qual a sua sugestão de texto? Se sim, justifique.

Quais itens ou trechos do documento exemplo de Política-Norma Correio Eletrônico você entende que precisam melhorar? Indique cinco. Justifique.

Quais itens ou trechos do documento exemplo Política-Norma Correio Eletrônico você entende que estão muito bons e você destacaria? Indique cinco. Justifique.

Documento Política-Norma de Uso da Internet

O Documento Política-Norma de Uso da Internet define os princípios básicos de segurança da informação definidos na Política Principal em relação ao uso da internet na organização.

Quando orientações básicas forem definidas neste documento, elas permitirão o desenvolvimento e a implantação de controles de segurança da informação e minimizarão os questionamentos sobre o que pode, o que não pode e o que é obrigatório em relação ao uso da internet.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. Caso existam serviços de uso de internet em ambientes diferentes e que necessitem de controles específicos, deverão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Este regulamento sobre uso da internet deve considerar e definir as regras para os seguintes elementos:

a. **Usuários**

Deve-se indicar os tipos de usuários que podem utilizar o serviço de uso de internet usando parcialmente ou totalmente recursos da organização.

Deve-se indicar as responsabilidades dos usuários em relação ao uso da internet.

b. **Serviços na internet**

Deve-se definir os serviços na internet que são permitidos e os que não são permitidos.

Talvez alguns serviços, como redes sociais, mereçam uma norma específica, considerando a quantidade de regras e orientações necessárias.

c. **Operacionalização**

Deve-se orientar sobre os procedimentos operacionais relativos à segurança, incluindo situações de erro e situações não previstas.

d. **Disponibilização de informações**

Deve-se definir (considerando aspectos de segurança) a disponibilização de informações pessoais e corporativas – e apenas corporativas. Deve-se lembrar que esses controles devem estar ligados a outros controles como, por exemplo: classificação da informação.

Exemplo prático de Política-Norma da Dimensão Uso da Internet

Utilização do ambiente internet pelo usuário

1. Objetivo

Definir os requisitos e regras de segurança para o uso do ambiente de internet, Intranet e Extranet da organização.

2. Abrangência

Esta política se aplica a todos os usuários (associados, prestadores de serviços e estagiários) que utilizam o ambiente de tecnologia da organização.

3. Implementação

A Gerência de Segurança da Informação e a Área de Apoio ao Usuário Final são responsáveis pela implementação e continuidade dessa norma de segurança.

4. Política de segurança e proteção da informação

(Itens referentes à internet – Documento já publicado.)

O acesso da informação deve ser autorizado apenas para os usuários que necessitam desta para o desempenho das suas atividades profissionais na organização. Esse conhecimento do usuário deve ser utilizado apenas para o desenvolvimento e operacionalização do negócio da organização.

O ambiente de internet deve ser usado para o desempenho das atividades profissionais do usuário para a organização. Sites que não contenham informações que agreguem conhecimento profissional e para o negócio não devem ser acessados. Os acessos realizados nesse ambiente são monitorados pela organização com o objetivo de garantir o cumprimento dessa política.

Os recursos de tecnologia da organização, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais. A utilização dos recursos de tecnologia, com finalidade pessoal, é permitida, desde que seja em nível mínimo e que não viole a Política de Segurança e Proteção da Informação e o Código de Conduta e Ética da organização Brasil.

A utilização das informações do ambiente de tecnologia ou do ambiente convencional pelos usuários da organização deve estar de acordo com os documentos institucionais "Código de Conduta", "Política de Privacidade – Dados Pessoais" e "Conduta Ética e Conflito de Interesses". Todos os usuários devem conhecer e entender esses documentos.

5. Definições

Internet

É o ambiente virtual onde diferentes computadores de várias partes do mundo se comunicam através de protocolos padrões, permitindo a troca de informações e o compartilhamento de conhecimento. Existem vários serviços disponibilizados na Internet, sendo o correio eletrônico e o ambiente gráfico www (World Wide Web) os mais conhecidos.

Intranet

É um ambiente semelhante ao da internet, porém restrito ao ambiente de tecnologia da organização.

Extranet

É o ambiente com o mesmo conteúdo da Intranet, porém extensivo ao ambiente da rede corporativa da organização, pela internet. Esse ambiente está logicamente restrito aos usuários organização.

Ambiente web

É o conjunto dos ambientes Internet, Intranet e Extranet.

Site

É o local virtual onde se encontram as informações relativas a um endereço do ambiente web. No mundo real é suportado por um ou vários equipamentos, que estão ligados à rede dentro do ambiente considerado.

6. Regras para os usuários

6.1. Apenas os softwares e versões homologados para a função de navegadores no ambiente web devem ser utilizados pelos usuários.

6.2. Todos os arquivos recebidos a partir do ambiente da internet para o ambiente do computador do usuário devem ser analisados por produto antivírus homologado para a organização.

6.3. O usuário não deve alterar a configuração do navegador da sua máquina no que diz respeito aos parâmetros de segurança. Havendo necessidade, o Help Desk deve ser acionado para informar o procedimento a ser seguido.

6.4. Quando estiver acessando a internet, o usuário não deve acessar sites ou executar ações que possa infringir direitos autorias, marcas, licença de software ou patentes existentes.

6.5. Nenhum material com nível de sigilo “Confidencial” ou superior pode ser disponibilizado fora das áreas seguras da Intranet.

6.6. Não são permitidas páginas pessoais de usuários ou qualquer outra propaganda comercial pessoal no ambiente web utilizando recursos da organização.

6.7. Nenhum material ofensivo ou hostil pode ser disponibilizado nos sites da organização no ambiente web.

6.8. É proibido e considerado abuso:

A visualização, transferência, cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo pornográfico ou relacionados a sexo, bem como a distribuição, interna ou externa, de qualquer tipo de conteúdo proveniente desses sites;
- Que defendam atividades ilegais;
- Que menosprezam, depreciam e incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, religião, nacionalidade;
  - A transferência ou cópia de grandes quantidades de arquivos de vídeo, som ou gráficos, não relacionados aos interesses de negócios da companhia. Esse tipo de ação afeta diretamente os recursos de rede;
  - Participação em:
    - Salas de chat ou grupos de discussão de assuntos não relacionados aos negócios da companhia;
    - Qualquer discussão pública sobre os negócios da companhia, através do uso de salas de chat, grupos de discussão, ou qualquer outro tipo de fórum público, a menos que autorizado pela Diretoria.
  - Distribuição de informações confidenciais da organização.

7. Conclusão

O não cumprimento das regras descritas neste documento que complementam a Política de Segurança e Proteção da Informação constitui falta grave, e o usuário está sujeito à penalidades administrativas e/ou contratuais.

Situações não previstas e sugestões devem ser encaminhada à Gerência de Segurança da Informação.

Dúvidas e informações adicionais poderão ser encaminhadas diretamente ao Help Desk.

Exercício de fixação
Uso da internet

Na sua organização, em relação ao uso da internet, existem regras diferentes para tipos de usuários diferentes? Indique os usuários considerados e os que na sua opinião deveriam ser considerados.

Quais itens ou trechos do documento exemplo de Política-Norma Uso da Internet você entende que precisam melhorar? Indique cinco. Justifique.

Quais itens ou trechos do documento exemplo Política-Norma Uso da Internet você entende que estão muito bons e você destacaria? Indique cinco. Justifique.

Documento Política-Norma Equipamentos de Tecnologia da Informação – recurso computacional

O Documento Política-Norma de Uso de Recurso Computacional define os princípios básicos de segurança da informação definidos na Política Principal em relação ao uso de equipamentos de tecnologia da informação.

Quando orientações básicas forem definidas neste documento, elas permitirão o desenvolvimento e a implantação de controles de segurança da informação e minimizarão os questionamentos sobre o que pode, o que não pode e o que é obrigatório em relação ao uso de recursos computacionais da organização e do usuário, no contexto dos serviços da organização.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. Caso existam situações de uso de recursos computacionais em ambientes diferentes e que necessitem de controles específicos, deverão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Este regulamento sobre Uso de Recursos Computacionais deve considerar e definir as regras para os seguintes elementos:

a. **Usuários**

Deve-se indicar os tipos de usuários que podem utilizar o serviço de Uso de Recursos Computacionais, usando parcialmente ou totalmente recursos da organização.

Deve-se indicar as responsabilidades dos usuários em relação ao Uso de Recursos Computacionais.

b. **Tipos de recursos**

Deve-se definir quais os tipos de recursos estão submetidos a este regulamento.

Talvez alguns tipos de recursos, como telefones inteligentes, mereçam uma norma específica, considerando a quantidade de regras e orientações necessárias.

c. **Operacionalização**

Deve-se orientar sobre os procedimentos operacionais relativos a segurança, incluindo-se aqui as situações de erro e situações não previstas.

d. **Uso de programas autorizados para cada recurso**

Deve-se definir os programas e ambientes que são autorizados para serem utilizados pelos recursos computacionais considerados neste regulamento.

e. **Controles de proteção técnica**

Deve-se definir nesta política-norma quais são os métodos de proteção aplicáveis aos recursos computacionais considerados neste regulamento.

f. **Uso de recursos corporativos e pessoais**

Deve-se definir o uso de recursos da organização e a possibilidade (ou não) de recursos pessoais acessando-utilizando informações da organização.

Exemplo prático de Política-Norma de Uso de Equipamento de Tecnologia da Informação – recurso computacional

Uso de recurso computacional

1. Objetivo deste regulamento

Definir os requisitos e as regras de segurança para a utilização do recurso computacional computador de mesa e computador portátil disponibilizado pelo ambiente de tecnologia utilizado pela organização.

2. Abrangência deste regulamento

Este regulamento se aplica a todos os usuários que utilizam as informações do ambiente de tecnologia da organização.

Este regulamento está alinhado com o regulamento "Política de Segurança e Proteção da Informação".

3. Implementação deste regulamento

O Departamento de Segurança da Informação, a Unidade de Segurança da Informação, o PRESTADOR e as chefias das áreas da organização desenvolverão ações contínuas e necessárias para a implementação deste regulamento, ficando o Departamento de Segurança da Informação responsável pela coordenação dessas ações.

4. Definições

As definições de termos relativos à Segurança da Informação estão descritas no regulamento "Definições Utilizadas em Segurança da Informação".

5. Política e regras

5.1. O recurso tipo computador, seja de mesa ou portátil, disponibilizado para o Usuário Profissional, é de propriedade da organização por meio de seus diversos órgãos.

5.2. O Usuário é o gestor desse recurso e deve garantir a sua integridade e perfeito funcionamento.

5.3. Ao deixar de trabalhar em determinada área da organização, em função de transferência para outra área, o recurso computador deve ficar na área de origem, salvo se existir um prévio acerto entre as partes.

5.4. Cada computador portátil que permanecer nas instalações de uma área da organização quando o usuário não estiver desempenhando suas atividades profissionais nessas instalações deve ser guardado em lugar seguro que possa ser trancado (exemplo: gaveta de escrivaninha ou armário).

5.5. Durante períodos de não funcionamento do ambiente de trabalho (exemplo: noite ou feriados) o pessoal de segurança, ou o equivalente local, registrará os computadores tipo portátil não protegidos adequadamente e manterá sob sua guarda, deixando um aviso no local, até que o respectivo associado procure o seu equipamento.

5.6. Ao viajar com um computador tipo portátil, o usuário deve:

- Manter o computador tipo portátil sempre consigo; e
- Ao tomar um táxi, certificar-se de que desceu com toda a sua bagagem, inclusive o computador.

5.7. Ao transportar o computador tipo portátil no carro, ele deve ser colocado sempre no porta-malas, onde não ficará visível. Não deixar o computador tipo portátil no veículo quando ele estiver estacionado.

5.8. O transporte do computador tipo portátil nas ruas já está sendo bastante visado pelos criminosos. Nesse caso, deve-se ser discreto, observar o ambiente ao redor e fazer o caminho mais seguro para onde se está dirigindo.

5.9. É responsabilidade de cada usuário dos sistemas da organização assegurar a integridade do computador e a confidencialidade das informações contidas nele.

5.10. Em nenhuma hipótese o associado poderá alterar a configuração do computador portátil, como por exemplo trocar o disco rígido, retirar ou acrescentar memória. Apenas a área técnica da organização está autorizada a realizar essa atividade.

5.11. Em caso de perda de acessório (exemplo: secure-id, mala ou mouse), o associado será responsável pelo seu pagamento.

6. Conclusão

O não cumprimento deste regulamento e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui falta grave, e o usuário está sujeito à penalidades administrativas e/ou contratuais.

Situações de exceção e não previstas deverão ser definidas pelo Departamento de Segurança da Informação e pela Unidade de Segurança da Informação da organização.

5

Política-Norma Dimensão Classificação da Informação, Política-Norma Dimensão, Desenvolvimento/ Aquisição de Sistemas Aplicativos, Política-Norma Dimensão Plano de Continuidade e Política-Norma Dimensão Cópias de Segurança

objetivos

Conhecer os componentes que devem ser considerados em uma Política-Norma Dimensão Classificação da Informação; Ter contato com os componentes que devem ser considerados em uma Política-Norma Dimensão Desenvolvimento/Aquisição de Sistemas Aplicativos; Aprender sobre os componentes que devem ser considerados em uma Política-Norma Dimensão Plano de Continuidade; Conhecer os componentes que devem ser considerados em uma Política-Norma Dimensão Cópias de Segurança.

conceitos

Política-Norma Dimensão Classificação da Informação; Política-Norma Dimensão; Desenvolvimento/Aquisição de Sistemas Aplicativos; Política-Norma Dimensão Plano de Continuidade; Política-Norma Dimensão Cópias de Segurança.

Documento Política-Norma da Dimensão Classificação da Informação

O Documento Política-Norma da Dimensão Classificação da Informação define os princípios básicos de segurança da informação para os padrões de confidencialidade ou sigilo da informação. Esses padrões são necessários para a existência de procedimentos padrões para o tratamento da informação e dos recursos de informação.

A Dimensão Classificação da Informação definirá ações em relação aos recursos de informação, como a guarda da informação, descarte da informação, critérios de criptografia para quando ocorrer a transmissão da informação de um certo padrão de sigilo e outras ações similares.

O objetivo da classificação da informação é definir como o usuário deve tratar a informação ou o recurso informação. Devem ser definidas regras de como uma informação deve ser guardada, se a informação precisa ser destruída após o seu uso e, se for destruída, qual a potência desta destruição.

Muitas pessoas confundem esse padrão de classificação da informação com a questão do controle de acesso à informação. Pensam erroneamente que, ao classificar uma informação como secreta, estará restringindo o acesso à informação e garantindo o correto uso da informação. A Dimensão Controle de Acesso à Informação (acesso lógico ou acesso físico) é o conjunto de controles que define quais usuários deverão ter acesso (ou não) à informação, independentemente da sua classificação de sigilo.

A Classificação da Informação influencia várias outras dimensões: por exemplo, o texto de uma mensagem de correio eletrônico será criptografado (ou não) pelo simples fato de ser uma mensagem para o mundo externo da organização. Este texto será criptografado se a informação em questão tiver sido classificada em um padrão de sigilo que exige que quando essa informação for sair do ambiente da organização, ela obrigatoriamente será criptografada.

Outra questão que os profissionais de segurança da informação enfrentam quando vão definir regras de classificação da informação é em relação à quantidade de padrões de sigilo. Normalmente varia de três a seis padrões. Quanto mais padrões, mais detalhada fica essa classificação, porém mais complexa para o usuário internalizar. Quanto menos complexa, mais fácil de o usuário internalizar, porém com menos detalhes. Essa quantidade de padrões é uma decisão da organização, porém deve-se considerar se a organização está submetida a alguma legislação sobre o assunto.

Outra questão a ser definida é o grau de granularidade para essa classificação.
Os profissionais de tecnologia da informação costumam promover grandes debates sobre essa granularidade: arquivo, base de dados, registro, campo, bit, byte etc.
Entende-se que quem vai avaliar e definir esse padrão de classificação da informação será o Gestor da Informação, que normalmente será de área não Tecnologia da Informação. Esse Gestor da Informação não entende detalhes de tecnologia da informação, mas entende de: relatório, transação, tela e similares. Portanto, a granularidade da informação para essa classificação deverá ser composta por elementos que o Gestor da Informação entenda. Em resumo, a granularidade deve ser em um padrão que o Gestor da informação compreenda.

Uma característica que o profissional de segurança da informação encontrará quando implantar esse controle de segurança, a classificação da informação, é a dos sistemas legados. Vamos generalizar: as informações legadas. Porque podemos ter "sistemas" legados de informações em recursos físicos. Evidentemente que após a formalização do Regulamento de Classificação da Informação todas as informações da organização deverão estar (ou tornarem-se) classificadas em relação ao seu padrão de sigilo. Porém, haverá maior dificuldade com as informações legadas. Em muitos casos, os sistemas legados nunca serão atualizados (sofrerão manutenção) para implantar o padrão de classificação da informação. Esse fato não acontecerá por dificuldades nos padrões de sigilo, mas por limitações da organização em dar manutenção em sistemas antigos, que em algumas situações não têm mais profissionais com competência para fazer a manutenção (o último profissional aposentou-se) ou em situações piores: não existe mais o programa fonte para permitir essa manutenção.

O importante é que a classificação de sigilo exista e a sua implantação aconteça conforme o ritmo possível para a organização.

Quando orientações básicas forem definidas neste documento, elas permitirão o desenvolvimento e a implantação de controles de segurança da informação e minimizarão os questionamentos sobre como deve ser a classificação de sigilo da informação e quais são as atividades obrigatórias para cada tipo de classificação.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia e ambiente físicos. Caso existam ambientes específicos que exigirão classificação específica, poderão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2. Porém, entendemos que a Dimensão Classificação da Informação deve ser a dimensão que menos subníveis de regulamentos terá.

Este regulamento sobre Classificação da Informação deve considerar os seguintes elementos:

a. **Legislação ou regras corporativas**

Deve-se verificar se a organização está submetida a alguma legislação ou regra corporativa e nesse caso é obrigada a adotar um determinado padrão de sigilo.

b. **Tipos ou quantidade de padrões de sigilo da informação**

Deve-se considerar a quantidade de tipos de padrões de classificação de sigilo da informação. Quanto mais padrões, mais detalhada fica essa classificação, porém mais complexa para o usuário internalizar. Quanto menos, mais fácil de o usuário internalizar, porém com menos detalhes. Essa quantidade de padrões é uma decisão da organização, que deve considerar se esta está submetida a alguma legislação.

c. **Começar em um projeto-piloto**

Caso a organização não possua a Dimensão de Classificação da Informação, sugiro que após todas as definições esses critérios sejam implantados em um projeto-piloto. Isso se recomenda em função de que a Dimensão de Classificação da Informação impacta várias outras dimensões. Um erro inicial ou a definição de um padrão não muito feliz pode ser mais facilmente corrigido em um projeto-piloto antes de esta regra ser obrigatória em toda a organização.

d. **Ambiente da organização: limitações e características**

Avalie o ambiente da organização em relação aos sistemas legados, ambiente físico e possibilidade de implantação desse conceito nos novos sistemas aplicativos. Essa análise é importante para ser feito um planejamento do uso efetivo da classificação.

Exemplo prático de Política-Norma da Dimensão Classificação da Informação

Classificação da informação – Padrão de Sigilo

1. Objetivo

Definir o conceito e estabelecer os critérios relativos à classificação da informação.

2. Escopo

Todos os usuários da informação da organização.

3. Introdução

Os Níveis de Classificação (NC) apresentados permitem que a informação possa ser identificada como:

- Pública;
- Interna;
- Confidencial;
- Restrita.

Todos os relatórios de sistemas, relatórios elaborados no ambiente de automação de escritório e todas as telas de sistemas deverão indicar o nível de classificação da informação referente à tela ou ao relatório.

Toda e qualquer outra forma de exposição da informação da organização deve ser classificada e ter explícito o seu nível de confidencialidade.

Essa indicação do nível de classificação deve ser colocada no rodapé ou no cabeçalho de cada página do relatório ou na tela. No caso de correio eletrônico, deve-se colocar em negrito na primeira linha do texto.

Para essa classificação, não foi considerado o seu tempo de validade. Sendo assim, a informação continuará sempre no nível indicado, até que o Gestor indique um novo nível de confidencialidade.

4. Definições

Classificação da informação

É a definição do nível de confidencialidade da informação, considerando: que procedimentos de proteção da informação devem ser seguidos.

Indicação de parâmetro opcional ou obrigatório

Os parâmetros descritos na sintaxe do nível de classificação da informação podem ser opcionais ou obrigatórios.

- (“parâmetro”): opcional;
- (parâmetro): obrigatório.

Usuários da organização

Indica associados, prestadores de serviço e estagiários que desenvolvem serviços internamente na organização e necessitam de informações da organização para a realização de suas atividades profissionais.

5. Classificação informação pública

5.1. Descrição

A informação classificada como “Pública” pode ser acessada por:

- Usuários organização;
- Organizações clientes e prestadoras de serviço;
- Público em geral.

Essa classificação se aplica, normalmente, às informações corporativas da organização que podem ser divulgadas para o público e para os clientes.

As informações sem classificação serão consideradas como “Pública”.

5.2. **Sintaxe**

A sintaxe dessa classificação é: Informação Pública.

5.3. **Exemplo**

Informação Pública:

- **Internamente**: qualquer usuário da organização;
- **Externamente**: qualquer pessoa.

5.4. **Cópia**

Pode ser copiada para fins comerciais e de conhecimento interno na organização.

5.5. **Guarda Física**

Sem restrições.

5.6. **Malote interno**

Não necessita fechar em envelope ou embrulho.

5.7. **Correio convencional**

- Não necessita fechar em envelope ou embrulho;
- Pode ser enviado como impresso;
- Usar correspondência simples.

5.8. **Correio Eletrônico**

Sem restrições.

5.9. **Destruição**

Normal. Sem procedimento especial.

5.10. **Fax**

Sem restrições.

6. Classificação informação interna

6.1. **Descrição**

A informação classificada como “Interna organização” indica que ela somente deve ser acessada por usuários da organização ou de áreas organizacionais explicitadas.

Ela se aplica normalmente a informações da organização que não possuem segredo de negócio ou que não comprometem a imagem da organização.

6.2. **Sintaxe**

A sintaxe dessa classificação é: Informação Interna organização (“área”).

6.3. **Exemplos**

Informação Interna Organização.

- **Internamente**: qualquer usuário organização;
- **Externamente**: não autorizado.

Informação Interna organização (Dir. Operações/Recebimento)

- **Internamente**: qualquer usuário da área de Recebimento da Diretoria de Operações;
- **Externamente**: não autorizado.

6.4. **Cópia**

Pode ser copiada para fins de conhecimento interno na organização.

6.5. **Guarda Física**

Dentro do ambiente de escritório da organização. Não necessita ser mantida trancada quando não estiver sendo usada.

6.6. **Malote interno**

Fechar em envelope ou embrulho. Não precisa indicar o nível de classificação.

6.7. **Correio convencional**

- Fechar em envelope ou embrulho sem identificação do nível de classificação da Informação;
- Utilizar correspondência simples.

6.8. **Correio Eletrônico**

Enviar sem proteção.

6.9. **Destruição**

Normal. Sem procedimento especial.

6.10. **Fax**

Sem restrições.

7. Classificação informação confidencial

7.1. **Descrição**

A informação classificada como "Confidencial" indica que esta possui forte restrição de uso, tem nível de confidencialidade maior que Interna e somente pode ser acessada por usuários:

- Da organização;
- Ou da organização e por pessoal do parceiro (cliente, prestador de serviço e outro).

A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização e/ou ao negócio do parceiro.

Caso se deseje que apenas determinadas áreas organizacionais da organização tenham direito a acessar essa informação, haverá indicação. Caso nenhuma área seja indicada, todas as áreas da organização poderão ter acesso a essa informação.

Em relação ao parceiro, é obrigatório a indicação da organização ou da organização e sua área específica.

7.2. **Sintaxe**

A sintaxe dessa classificação é: Informação Confidencial organização ("área")/parceiro (organização).

7.3. **Exemplos**

Informação Confidencial organização:

- **Internamente**: todos os usuários;
- **Externamente**: não autorizado.

Informação Confidencial organização (Diretoria Operações):

- **Internamente**: todos os usuários da área organizacional Diretoria de Operações;
- **Externamente**: não autorizado.

Informação Confidencial organização/parceiro (Rede ABC):

- **Internamente**: qualquer usuário organização;
- **Externamente**: por pessoal da empresa Rede ABC.

Informação Confidencial organização (Financeiro/Gerentes, Marketing)/Parceiro (Rede Bola/Marketing):

- **Internamente**: usuários Gerentes da Área Financeira + pessoal da Área de Marketing;
- **Externamente**: pessoal da área de Marketing da empresa Rede Bola.

Informação Confidencial organização/parceiro (clientes da região Nordeste):

- **Internamente**: qualquer usuário organização;
- **Externamente**: organizações clientes da região Nordeste.

7.4. **Cópia**

Pode ser copiada para fins comerciais e de conhecimento interno na organização.

7.5. **Guarda Física**

Deve ser mantida trancada quando não estiver sendo usada.

7.6. **Malote interno**

Fechar em envelope ou embrulho com a marca da classificação Informação Confidencial organização/parceiro e seu detalhamento.

7.7. **Correio convencional**

- Fechar em envelope ou embrulho com a marca da classificação Informação Confidencial organização ou parceiro, e seu detalhamento;
  - Colocar o envelope ou embrulho no interior de um outro envelope sem classificação;
- O Gestor deve avaliar uso de correspondência simples, tipo Sedex ou outro.

7.8. **Correio Eletrônico**

- Origem ou destinatário é um endereço, não a organização:
  - Enviar como arquivo em anexo cifrado com senha;
  - Enviar senha por outro meio de comunicação;
  - Utilizar certificação digital assim que estiver disponível.
- Origem e destinatário são endereços organização (organização.com.br):
  - Normal, sem restrições.

7.9. **Destruição**

Internamente: destruir sob supervisão da organização, de modo a assegurar a eliminação completa da informação.

No parceiro: a organização deve orientar o parceiro a destruir essa informação de forma supervisionada, de modo a assegurar a eliminação completa da informação.

7.10. **Fax**

Somente com a autorização do Gestor dessa informação. No caso de relatórios elaborados no ambiente de automação de escritório, somente com a autorização do autor do relatório.

8. Classificação informação restrita organização (pessoas)

8.1. **Descrição**

A informação classificada como "Restrita organização" indica que esta somente pode ser acessada por usuário da informação da organização explicitamente indicado pelo nome ou por área organizacional a que pertence.

A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

É obrigatória a indicação do grupo ou das pessoas que podem acessar essa informação.

8.2. **Sintaxe**

A sintaxe dessa classificação é:

Informação Restrita organização (pessoas)

8.3. **Exemplos**

Informação Restrita organização (Antônio Potiguar, José da Silva, Maria Iracema)

- **Internamente**: apenas os usuários Antônio Potiguar, José da Silva e Maria Iracema;
- **Externamente**: não autorizado.

Informação Restrita organização (Presidente, Diretoria).

Internamente: apenas o presidente e diretores da organização).

8.4. **Cópia**

Não pode ser copiada. Deve ser sempre enviada pelo Gestor.

8.5. **Guarda Física**

Deve ser mantida trancada quando não estiver sendo usada.

8.6. **Malote interno**

Fechar em envelope ou embrulho com a marca da classificação Informação Restrita organização e seu detalhamento.

8.7. **Correio convencional**

- Fechar em envelope ou embrulho com a marca da classificação Informação Restrita organização e seu detalhamento;
- Colocar o envelope ou embrulho no interior de um outro envelope sem classificação;
- Utilizar serviço de correspondência Sedex ou equivalente.

8.8. **Correio Eletrônico**

- Origem ou destinatário é um endereço não organização:
  - Enviar como arquivo em anexo cifrado com senha;
  - Enviar senha por outro meio de comunicação;
  - Utilizar certificação digital assim que estiver disponível.

- Origem e destinatário são endereços organização (organização.com.br):
  - Normal, sem restrições.
- Deve-se criar uma lista de distribuição contendo os nomes dos destinatários, para evitar o envio indevido de email, por erro, para usuário não autorizado a receber essa informação.

8.9. **Destruição**

Destruir sob supervisão da organização, de modo a assegurar a eliminação completa da informação.

8.10. **Fax**

Não enviar informação classificada nesse nível através de fax.

9. Conclusão

As situações específicas devem ser registradas junto à Gerência de Segurança da Informação.

A alteração dos relatórios e telas dos sistemas deverão acontecer ao longo dos próximos meses.

Os novos relatórios e as novas telas deverão ser implantados contendo explícito esse Nível de Confidencialidade da informação atribuído pelo Gestor.

Quando de situações de manutenção, deve-se aproveitar a alteração a ser feita para a inclusão dessa classificação.

Situações não previstas e dúvidas devem ser encaminhadas à Gerência de Segurança da Informação.

Exercícios de fixação
Classificação da Informação, Desenvolvimento-Aquisição Aplicativos, Plano de Continuidade, Cópias de Segurança e Gestão de Riscos

Sua organização possui Políticas-Normas de Classificação da Informação, Desenvolvimento/Aquisição de Sistemas Aplicativos, Plano de Continuidade, Cópias de Segurança e Gestão de Riscos?

Se sim, explique o grau de efetividade desses regulamentos.

Se não, o que a falta desses regulamentos impacta no Processo Organizacional de Segurança da Informação?

Sua organização está submetida a alguma lei ou regra corporativa sobre algum desses assuntos?

Considere os regulamentos Políticas-Normas de Classificação da Informação, Desenvolvimento/Aquisição de Sistemas Aplicativos, Plano de Continuidade, Cópias de Segurança e Gestão de Riscos.

Qual a prioridade de implantação você recomendaria para uma organização? Justifique.

Exercício de fixação – Classificação da Informação

Quais itens ou trechos do documento exemplo de Política-Norma Classificação da Informação você entende que precisam melhorar? Indique cinco. Justifique

Quais itens ou trechos do documento exemplo Política-Norma Classificação da Informação você entende que estão muito bons e você destacaria? Indique cinco. Justifique.

Documento política-norma da dimensão desenvolvimento/aquisição de sistemas aplicativos

O Documento Política-Norma para a Dimensão de Desenvolvimento e/ou Aquisição de Sistemas Aplicativo define os controles relacionados à segurança da informação que devem ser considerados quando a organização desenvolve, ou encomenda o desenvolvimento, ou adquire sistemas aplicativos.

Quando as orientações básicas forem definidas nesse documento, elas permitirão o desenvolvimento e a implantação de controles de segurança da informação e minimizarão os questionamentos sobre o que pode, o que não pode e o que é obrigatório, considerando a segurança da informação em relação ao desenvolvimento ou aquisição de sistemas aplicativos.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. Caso existam detalhes referentes ao desenvolvimento de sistemas aplicativos em ambientes diferentes e que necessitem de controles específicos, deverão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Esse regulamento sobre os controles de segurança da informação para o desenvolvimento ou uso de sistemas aplicativos deve considerar e definir as regras para os seguintes elementos:

a. **Continuidade do serviço do desenvolvedor**

Deve-se ter a garantia de que o desenvolvimento e manutenção de sistemas (interno ou externo) terá continuidade ao longo do tempo de vida da organização.

b. **Requisitos de segurança da informação**

Nessa fase de desenvolvimento ou aquisição deve-se definir os critérios que serão utilizados pelos diversos controles de segurança da informação. Essas definições, ocorrendo neste momento de desenvolvimento ou de aquisição, minimizarão ou evitarão problemas futuros. Por exemplo, deve-se definir o tempo de indisponibilidade do sistema em desenvolvimento--aquisição neste momento. Caso não seja feita essa tarefa, a organização terá de fazer posteriormente uma avaliação de impacto no negócio em caso de parada dos sistemas para identificar o tempo máximo de indisponibilidade que a organização suporta.

Pode ser que a exigência identificada necessite de alterações inclusive, em arquitetura técnica da tecnologia da informação.

Deve-se definir:

- Como será a identificação do usuário?
- Quem será o Gestor da Informação?
- Qual será o tempo máximo de indisponibilidade do sistema?
- Quem ou que área será o custodiante da informação?
- Quais são os requisitos para as cópias de segurança?
- Quais são as exigências para o registro de acesso à informação?

Exemplo prático de Política-Norma da Dimensão Desenvolvimento/Aquisição de Sistemas Aplicativos

Desenvolvimento e manutenção de sistemas

1. Objetivo deste regulamento

Definir os requisitos e as regras de segurança que devem ser considerados quando do desenvolvimento e manutenção de sistemas desenvolvidos pelo ou para a organização.

2. Abrangência deste regulamento

Este regulamento se aplica a todos os sistemas desenvolvidos pela organização ou os sistemas desenvolvidos para a organização por prestadores de serviço terceiros.

Este regulamento está alinhado com o regulamento "Política de Segurança e Proteção da Informação."

3. Implementação deste regulamento

O Departamento de Segurança da Informação, a Unidade de Segurança da Informação e as chefias das áreas da organização desenvolverão ações contínuas e necessárias para a implementação deste regulamento, ficando o Departamento de Segurança da Informação responsável pela coordenação dessas ações.

4. Definições

As definições de termos relativos à Segurança da Informação estão descritas no regulamento "Definições Utilizadas em Segurança da Informação".

5. Política e regras

Quando do desenvolvimento ou manutenção de sistemas de informação, os aspectos de segurança a seguir descritos devem ser formalmente definidos pelo desenvolvedor e acordados com o Gestor da Informação. A Unidade de Segurança da Informação validará esse processo de controle.

5.1. **Continuidade do serviço**

Exigência de tempo para a recuperação do sistema de informação, caso ocorra uma situação de indisponibilidade dos recursos de informação. Essa definição deve considerar uma avaliação de impacto financeiro, operacional e de imagem nos serviços prestados pela organização.

5.2. **Criptografia da informação**

Definição das informações que serão criptografadas, quando forem transmitidas ou armazenadas.

5.3. **Acesso à informação**

5.3.1. **Identificação**

Definição de como será a identificação do usuário, quando do acesso ao sistema de informação

5.3.2. **Autenticação**

Definição de como será a autenticação do usuário quando for acessar o sistema de informação.

5.3.3. **Transação do Gestor da Informação**

Definição de qual será e como será a transação a ser executada pelo Gestor da Informação, quando houver procedimento de liberação da informação para o usuário.

5.3.4. **Grupos de usuário**

Definição se será possível a liberação de acesso à informação através de perfil de acesso em grupo

5.3.5. **Registro das ações realizadas com a informação**

Definição do tempo de guarda dos registros realizados, quando do acesso e da utilização da informação.

5.4. **Cópias de segurança**

Definição do tempo de guarda das cópias de segurança da informação. Devem ser considerados os seguintes aspectos:

5.4.1. **Aspecto Legal**

Identificação dos requisitos exigidos pelos normativos legais.

5.4.2. **Aspecto Histórico**

Identificação da necessidade da organização em guardar a informação por motivos históricos.

5.4.3. **Aspecto de Auditoria**

Identificação da necessidade de guarda de cópia de segurança em função de requisitos de auditoria.

6. **Conclusão**

O não cumprimento deste regulamento e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui em falta grave e o usuário está sujeito à penalidades administrativas e/ou contratuais.

Situações de exceção e não previstas deverão ser definidas pelo Departamento de Segurança da Informação e pela Unidade de Segurança da Informação, considerando as áreas da organização envolvidas.

Exercício de fixação
Desenvolvimento-Aquisição de Sistemas Aplicativos

Quais itens ou trechos do documento exemplo de Política-Norma Desenvolvimento/Aquisição de Sistemas Aplicativos você entende que precisam melhorar? Indique cinco. Justifique.

Quais itens ou trechos do documento exemplo Política-Norma Desenvolvimento/Aquisição de Sistemas Aplicativos que você entende que estão muito bons e você destacaria? Indique cinco. Justifique.

Documento Política-Norma da Dimensão Plano de Continuidade

O Documento Política-Norma da Dimensão de Plano de Continuidade define os princípios básicos de segurança da informação para a existência do Plano de Continuidade de Negócios da organização para quando da indisponibilidade de informação ou de recurso de informação.

Quando orientações básicas forem definidas neste documento, elas permitirão o desenvolvimento e a implantação de controles de segurança da informação e minimizarão os questionamentos sobre o que deve ser realizado em relação à continuidade de negócios quando da indisponibilidade da informação ou de recursos de informação que impeçam a organização de atingir os seus objetivos corporativos.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. Caso existam características para os planos de continuidade em ambientes diferente e que necessitem de controles específicos, deverão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Este regulamento sobre Plano de Continuidade de Negócio deve considerar e definir as regras para os seguintes elementos:

a. **Escopo**

Deve-se indicar quais os ambientes o plano contempla.

b. **Responsabilidades**

Deve-se indicar quem ou que área é responsável

- Pela elaboração e manutenção do plano;
- Pela definição do tempo de indisponibilidade máxima dos recursos de informação.

c. **Teste do Plano**

Deve-se indicar a periodicidade para a realização dos testes, bem como quem ou que área tem a responsabilidade de conduzir e avaliar o teste.

Deve-se indicar os principais procedimentos e controles para a realização do teste.

d. **Manutenção do Plano**

Deve-se indicar como será feita a manutenção do plano e a sua periodicidade.

Exemplo prático de Política-Norma da Dimensão Plano de Continuidade

Continuidade operacional

1. **Objetivo deste regulamento**

Definir os requisitos e as regras de segurança para a continuidade operacional dos recursos de informação utilizados pela organização.

2. **Abrangência deste regulamento**

Este regulamento se aplica a todos os ambientes de tecnologia da organização e a todas as pessoas que utilizam essas informações.

Este regulamento está alinhado com o regulamento "Política de Segurança e Proteção da Informação."

3. **Implementação deste regulamento**

O Departamento de Segurança da Informação, a Unidade de Segurança da Informação e as chefias das áreas da organização desenvolverão ações contínuas e necessárias para a implementação deste regulamento, ficando o Departamento de Segurança da Informação responsável pela coordenação dessas ações.

4. **Definições**

As definições de termos relativos à Segurança da Informação estão descritas no regulamento "Definições Utilizadas em Segurança da Informação".

5. **Política e regras**

5.1. Os recursos de informação utilizados pela organização devem ter definido o seu nível de disponibilidade. Esse nível de disponibilidade será o direcionador para a solução de continuidade operacional referente aos serviços prestados existentes no ambiente de tecnologia da informação.

5.2. O Gestor da Informação é o responsável pelo nível de disponibilidade de cada informação ou serviço sob a sua custódia. Esse nível de disponibilidade deve ser validado pela Área de Tecnologia da Informação, analisando os requisitos técnicos necessários e possíveis para a implementação dessa solução.

5.3. O Gestor da Informação é responsável pelo custo de implantação da solução desenvolvida pela Área de Tecnologia da Informação para atender o nível de disponibilidade definido.

5.4. O desenvolvimento de planos de continuidade operacional para garantir o nível de disponibilidade da informação/serviço será coordenado pelo Departamento de Segurança da Informação, desenvolvido pela Unidade de Segurança da Informação ou por consultoria especializada e validado pelo Gestor da Informação.

5.5. Pelo menos uma vez por ano o plano de continuidade deve ser testado de forma estruturada, documentado e com possibilidade de ser auditado.

5.6. Os testes do plano de continuidade devem ocorrer com a participação das pessoas que provavelmente serão envolvidas, caso uma situação real acontecer.

5.7. Os recursos de informação alternativos e os processos utilizados em situação de contingência devem ter o mesmo nível de segurança, proteção e sigilo dos elementos utilizados em situação normal.

6. **Conclusão**

O não cumprimento deste regulamento e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui falta grave e o usuário está sujeito à penalidades administrativas e/ou contratuais.

Situações de exceção e não previstas deverão ser definidas pelo Departamento de Segurança da Informação e pela Unidade de Segurança da Informação, considerando as áreas da organização.

Exercício de fixação
Plano de continuidade

Quais itens ou trechos do documento exemplo de Política-Norma Plano de Continuidade você entende que precisam melhorar? Indique cinco. Justifique.

Quais itens ou trechos do documento exemplo Política-Norma Plano de Continuidade você entende que estão muito bons e você destacaria? Indique cinco.

Documento Política-Norma da Dimensão Cópias de Segurança

O Documento Política-Norma da Dimensão de Cópias de Segurança da Informação detalha os princípios básicos de segurança da informação definidos na Política Principal em relação às cópias de segurança da informação.

Quando orientações básicas forem definidas neste documento, elas permitirão a existência de cópias de segurança da informação e minimizarão os questionamentos sobre o que pode, o que não pode e o que é obrigatório para a existência dessas cópias.

O objetivo básico da existência de cópias de segurança é permitir à organização a sua continuidade no acesso à informação quando por algum motivo a informação principal for destruída.

Devem ser detalhados controles e regras que são comuns a todos os ambientes de tecnologia. Caso existam situações de cópias de segurança em ambientes diferentes e que necessitem de controles específicos, deverão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2.

Este regulamento sobre Cópias de Segurança da Informação deve considerar e definir as regras para os seguintes elementos:

a. **Regras para tipos de cópias**

Deve-se definir regras para a existência de cópias motivadas por questões:

- Perda da mídia que contém a informação original;
- Legais (estar em conformidade com a legislação);
- Históricas (a organização pretende guardar a informação mesmo que não tenha a obrigação legal para tal);
- Auditoria (a organização é submetida à auditorias que fazem exigências específicas).

b. **Definição de ciclo e periodicidade**

Devem ser definidos os ciclos e as periodicidades que obrigatoriamente devem ser cumpridas.

c. **Ambientes contemplados**

Deve-se indicar quais ambientes estão contemplados pela norma.

d. **Responsabilidades**

Devem ser definidas as responsabilidades em relação a:

- Execução das cópias de segurança;
- Validação se as cópias de segurança continuam válidas ao longo do tempo;
- Escolha e qualidade dos locais onde ficarão as cópias de segurança.

Exemplo prático de Política-Norma da Dimensão Cópias de Segurança

Cópias de segurança da informação

1. Objetivo deste regulamento

Definir os requisitos e as regras de segurança para a existência eficiente e eficaz das cópias de segurança para a informação armazenada, processada ou transmitida no ambiente de tecnologia utilizado organização.

2. Abrangência deste regulamento

Este regulamento se aplica a todos os usuários que utilizam as informações do ambiente de tecnologia da organização.

Este regulamento está alinhado com o regulamento "Política de Segurança e Proteção da Informação."

3. **Implementação deste regulamento**

O Departamento de Segurança da Informação, a Unidade de Segurança da Informação e as chefias das áreas da organização desenvolverão ações contínuas e necessárias para a implementação deste regulamento, ficando o Departamento de Segurança da Informação responsável pela coordenação dessas ações.

4. Definições

As definições de termos relativos à Segurança da Informação estão descritas no regulamento "Definições Utilizadas em Segurança da Informação".

5. Política e regras

5.1. Existência da cópia de segurança

Para cada informação ou grupo de informação, deve existir, de maneira estruturada e validada com o Gestor da Informação, regras e características das cópias de segurança a serem realizadas.

5.2. Cada cópia de segurança deve ter definida:

5.2.1. Periodicidade

Define de quanto em quanto tempo será feita uma cópia. Por exemplo, periodicidade semanal significa que a cada semana é feita uma cópia.

5.2.2. Ciclo

É o período em que a cópia fica válida e existirá. Exemplo, se temos uma periodicidade mensal e um ciclo anual, significa que a cada mês temos uma cópia que fica guardada por 12 meses. Em janeiro de 2012, a cópia de janeiro de 2011 será descartada, sendo substituída pela cópia de janeiro de 2012.

5.2.3. Cópias específicas

Algumas vezes o sistema (ou ambiente) não é atendido pelas cópias normais que estão planejadas. Nesse caso, é necessário uma cópia específica.

Outra situação que pode gerar cópias específicas é quando o ambiente está passando por um momento diferente, no qual uma cópia normal não atenderá ou atenderia usando muito tempo.

5.2.4. Tipo de execução de Cópia

Dependendo das facilidades do ambiente de tecnologia utilizado, podem existir cópias completas, cópias incrementais (totais ou somente para alterações).

Cada um desses tipos de cópias tem suas características que devem ser consideradas para a recuperação da informação.

5.3. Cópia principal – Ambiente físico

O ambiente físico onde ficam localizadas as cópias principais deve ser protegido adequadamente para que exista a garantia de que as informações armazenadas nas mídias continuam disponíveis. Deve haver:

- Controle de acesso físico;
- Acesso apenas de pessoal autorizado;
- Condições ambientais adequadas.

5.4. Cópia de segurança – Ambiente físico

O ambiente físico onde ficam localizadas as cópias de segurança deve ser protegido adequadamente para que exista a garantia de que as informações armazenadas nas mídias continuam disponíveis. Deve haver:

- Controle de acesso físico;
- Acesso apenas de pessoal autorizado;
- Condições ambientais adequadas.

5.5. **Unidade de guarda**

As mídias podem ir para o local externo em unidades que pode ser cada mídia isolada, ou as mídias do dia, ou outra forma de se empacotar essas mídias.

Essa unidade é importante para quando for descrito os procedimentos de recuperação, quando da ocorrência de situações de contingência.

5.6. **Capacidade da mídia: total e gravada**

Esse item permite identificar situações possíveis de economia de mídia, em situações onde se poderia gravar mais de um dia, por exemplo, numa mesma mídia, em vez de uma mídia para cada dia.

5.7. **Características da mídia**

- Capacidade de regravações;
- Exigência de condições ambientais;
- Outras características da mídia.

5.8. **Recuperação do ambiente/sistema**

Tempo desejado. Deve-se descrever aqui o tempo que se deseja que o ambiente deva se recuperar.

Tempo já avaliado: deve-se indicar o tempo de recuperação para o ambiente/sistema, já realizado em situações de testes ou situações reais.

5.9. **Necessidades de cópias**

5.9.1. **Informações para a recuperação do ambiente computacional**

São informações utilizadas para recuperar o ambiente computacional em função de alguma falha. Neste caso, quanto mais recente for a informação da cópia de segurança, melhor para a recuperação do ambiente. Para este tipo de necessidade, uma única cópia atende às necessidades de segurança.

5.9.2. **Informações legais**

São os dados que devem ser guardados em função de alguma legislação externa ou interna à companhia.

5.9.3. **Informações históricas**

São os dados que, mesmo não tendo obrigatoriedade de existir, a empresa deseja guardar para ter acesso a situações anteriores.

5.9.4. **Informações para auditoria**

São os dados da trilha de auditoria e do log, necessários para a execução de investigações e/ou auditorias.

5.10. **Exigências contratuais**

5.10.1. **Recuperação de informações**

São as exigências de contratos para que a organização recupere determinadas informações (históricas ou legais).

5.10.2. **Continuidade do negócio**

São as exigências contratuais que formalizam multas, caso o serviço prestado pela organização esteja indisponível durante período superior ao determinado contratualmente. Considerar que o ambiente/sistema em questão é fundamental para a continuidade do negócio.

5.11. **Existência de espelhamento**

- No site principal;
- No site alternativo.

A existência de espelhamento de dados no local externo é a melhor solução para a questão de cópias de segurança. Esse caso não implica na necessidade de não se ter cópias de segurança. Significa que os requisitos para essas cópias podem ser mais amenos.

5.12. **Dados a serem copiados**

- Todos;
- Parcial.

Deve-se definir quais são os dados que existirão nas cópias de segurança. Na maioria dos casos serão as mesmas informações do arquivo do ambiente principal.

Podem existir situações específicas que não exija a gravação de todos os dados do ambiente em produção. Um subconjunto dessas informações pode ser suficiente para atender requisitos para recuperação do ambiente computacional, de informações legais, de informações históricas e de informações para auditoria.

5.13. **Testes**

Neste item devem ser identificados os procedimentos para a realização de testes com o objetivo de se ter maior garantia de que os dados gravados na mídia continuam em condições de uso pela organização.

6. **Conclusão**

O não cumprimento deste regulamento e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui falta grave e o usuário está sujeito às penalidades administrativas e/ou contratuais.

Situações de exceção e não previstas deverão ser definidas pelo Departamento de Segurança da Informação e pela Unidade de Segurança da Informação, considerando as áreas da organização envolvidas.

6

Dimensão Conscientização e Treinamento do Usuário, Política-Norma Dimensão Conscientização e Treinamento do Usuário

objetivos

Conhecer a Dimensão de Treinamento e Conscientização do Usuário e sua relação com a Dimensão Política de Segurança da Informação; Aprender sobre os componentes que devem ser considerados em um Política-Norma Dimensão Conscientização e Treinamento do Usuário; Concluir o tema Políticas-Normas de Segurança da Informação.

conceitos

Dimensão de Conscientização e Treinamento do Usuário; Política-Norma Dimensão Conscientização e Treinamento do Usuário.

Dimensão conscientização e treinamento do usuário: introdução

A Dimensão de Conscientização e Treinamento do Usuário tem por objetivo realizar ações para que todos os usuários recebam o treinamento adequado para a sua conscientização e para a sua capacitação em relação às suas responsabilidades em relação à segurança da informação.

A implantação da política de segurança da informação deve ser suportada pela realização de treinamentos para a conscientização dos usuários. Nesses treinamentos os usuários terão conhecimento dos regulamentos que estão em implantação (ou já implantados) em segurança da informação; entenderão esses regulamentos e serão apresentados às suas responsabilidades perante o Processo Organizacional de Segurança da Informação.

O Tribunal de Contas da União, no Acórdão 1092/2007 – Plenário, recomenda:

"9.1.2. elabore, aprove e divulgue Política de Segurança da Informação – PSI conforme o estabelecido na NBR ISO/IEC 17799:2005, item 5.1.1;

9.1.4. crie mecanismos para que as políticas e normas de segurança da informação se tornem conhecidas, acessíveis e observadas por todos os funcionários e colaboradores da Empresa conforme o estabelecido na NBR ISO/IEC 17799:2005, item 5.1.1; (Brasil, TCU, 2012, página 45.)"

O DSIC recomenda na Instrução Normativa nº 02 (Metodologia de Gestão de Segurança da Informação e Comunicações) de 13 de Outubro de 2008, a implementação de programas de conscientização e treinamento.

As políticas e normas precisam existir, mas para elas se tornarem vivas e efetivas, precisam ser de conhecimento dos usuários e ser internalizadas por eles. Esse processo de conscientização e treinamento precisa acontecer em paralelo com a implantação dos regulamentos de segurança da informação ou um pouco depois.

Essa dimensão de treinamento e conscientização precisa ser contínua. Todos os usuários (funcionários, prestadores de serviço, estagiários, menor aprendiz, conselheiros e outros) precisam receber conscientização constante e serem formalmente treinados periodicamente.

Essa formalização se faz necessária para garantir que realmente o usuário fez o treinamento e para se ter evidências da ocorrência do treinamento, caso a organização precise atender a auditorias internas, externas ou de clientes.

Planejamento para o treinamento

O Gestor da Segurança da Informação é o responsável pelo andamento do Processo Organizacional de Segurança da Informação. Ele é quem movimenta todos os recursos da organização para que a segurança da informação aconteça.

Em relação ao treinamento de pessoas, essa ação deve ser feita em conjunto com a área de Recursos Humanos. Na realidade, o Gestor da Segurança da Informação deve fazer com que a segurança da informação seja mais um treinamento promovido pela organização. A área responsável por treinamentos, a área que conhece as melhores técnicas de treinamento, que conhece o funcionário, é a área de Recursos Humanos.

O escopo deste curso são os aspectos da segurança da informação, mas é importante que esteja alinhado que qualquer treinamento deve ser feito em conjunto com a área de Recursos Humanos. Inclusive a área de Recursos Humanos pode assumir a operacionalização do processo de treinamento e conscientização.

Consideramos as seguintes etapas para um efetivo treinamento e conscientização em segurança da informação:

a. **Identifique as políticas e normas de segurança da informação**

Identifique as políticas-normas de segurança da informação existentes e as que não existem. Utilize a Arquitetura de Segurança da Informação para melhor visualização.

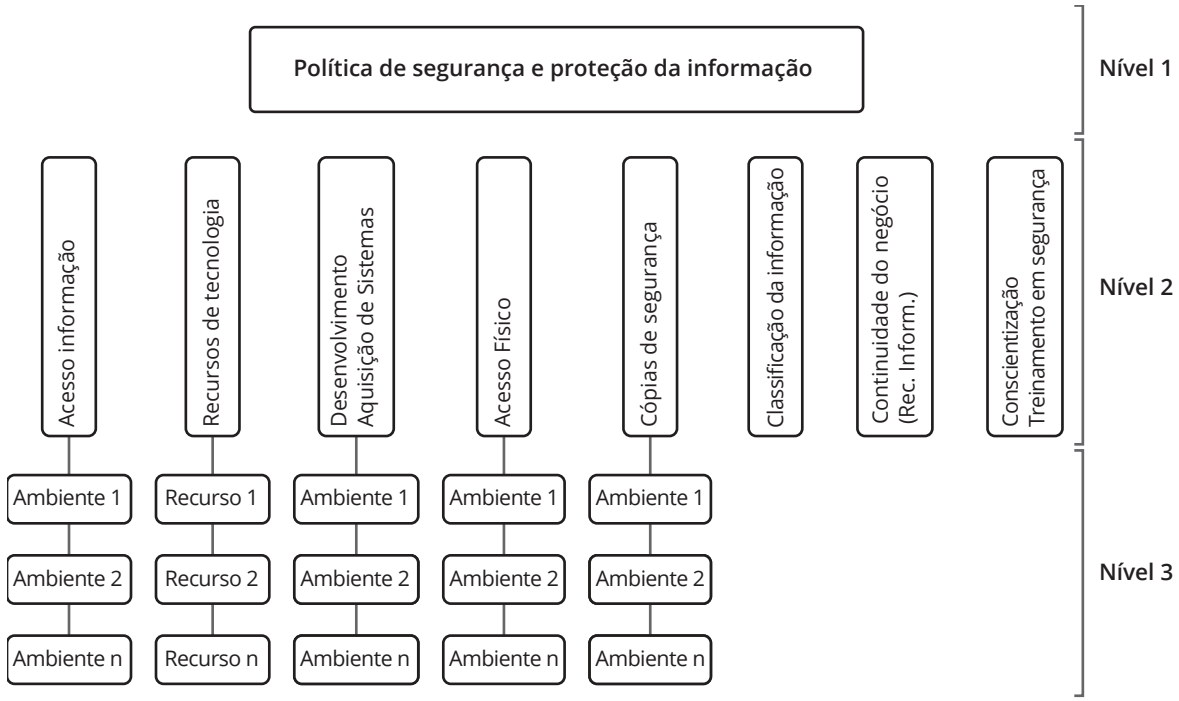


Figura 6.1 Estrutura da Arquitetura da Política de Segurança da Informação.

Verifique o impacto para o treinamento, o fato da não existência de alguns regulamentos. Identifique se já existem datas previstas para a existência desses regulamentos faltosos. Fale isso no treinamento. Explique, considerando cada tipo de usuário, o planejamento em segurança da informação.

b. **Identifique grupos de usuários**

Identifique tipos de grupos de usuários que têm responsabilidades e uso da informação diferentes.

Analise a necessidade de cada um desses grupos e verifique se será preciso apresentar sessões de treinamento diferentes para cada um desses grupos. Essa divisão por tipo de grupo deve estar ligada ao tipo de responsabilidade. Muitas vezes essa classificação vai coincidir com a hierarquia organizacional. Mas não tome a hierarquia organizacional como base, tome como base as responsabilidades.

c. **Defina os tipos de treinamentos que serão realizados**

Baseado nos grupos existentes, defina quantos tipos de treinamentos existirão. Pense em blocos e identifique, em cruzamento, o que cada um desses grupo de usuários precisam fazer como treinamento.

Por exemplo: podemos ter um bloco de treinamento básico de segurança. E podemos ter um bloco isolado para os gestores e executivos que vão receber novas responsabilidades. É conveniente a separação de treinamento para um grupo que terá apenas o treinamento básico daquele que terá o treinamento básico mais o treinamento de novas responsabilidades.

Analise e escolha como o treinamento acontecerá. Mais do que nunca, essa forma de treinamento deve estar totalmente alinhada à cultura da organização e com a maneira histórica que a organização promove treinamentos. Palestras presenciais, palestras gravadas, palestras transmitidas ao vivo, treinamento via computador e teatro corporativo ao vivo são alguns exemplos de se transmitir a mensagem da segurança da informação.

Em uma situação real que o autor deste livro viveu, no primeiro ano tivemos palestras presenciais, no segundo ano treinamento via computador e no terceiro ano o teatro corporativo. Cada organização tem a sua maneira mais adequada de realizar o treinamento.

d. **Considere todos os locais físicos**

Ao fazer seu planejamento para estimar o custo do treinamento, considere todos os locais físicos da organização. Não deve ser apenas os usuários do local do escritório principal que devem ter o melhor treinamento.

Todos os usuários devem ter o mesmo treinamento. E isso custa recursos. O processo de segurança custa recursos financeiros, de tempo, de exemplo gerencial e outros recursos indiretos. Da mesma maneira que é planejado um software seguro ou os planos de continuidade de negócio, é necessário planejar e executar treinamento para os usuários.

Todo treinamento bem feito realizado para os usuários tem um bom retorno. Dizem que as pessoas são o elo frágil da segurança, mas existem outras visões que afirmar que as pessoas são o elo mais forte da segurança.

Prepare o material do treinamento

Todas as ações que acontecerão no treinamento precisam estar rigorosamente planejadas. É recomendado gerar todo o material necessário com boa antecedência. Para organizações muito grandes, pode ser feito um treinamento-piloto.

Realize o treinamento

A realização do treinamento deve ter a mesma qualidade em todas as sessões de treinamento. Todos devem receber as mesmas orientações, considerando o seu tipo de usuário.

Mantenha o registro formal da participação de cada participante. Isso pode ser fundamental para os próximos treinamentos, para auditorias e para responder algum questionamento judicial.

Durante a realização de treinamento, costuma-se dar alguns brindes. A distribuição dos brindes deve ser compatível com o porte da organização. Através da quantidade e do tipo de brinde distribuído os usuários também vão avaliar o esforço e seriedade da organização em relação ao treinamento.

Não subestime a capacidade do usuário. O usuário é o recurso de informação que vai cristalizar o Processo Organizacional da Segurança da Informação.

Avalie o treinamento

Avalie o treinamento realizado, considerando a avaliação por todos os envolvidos. Evidentemente os usuários serão a principal voz de avaliação, porém considere a avaliação dos profissionais que realizaram palestras ou atividades similares.

Considere também receber avaliação do pessoal de infraestrutura e do pessoal de Recursos Humanos que acompanhou o treinamento. Enfim, todos que estiveram envolvidos no treinamento devem ser avaliados e devem avaliar o treinamento como um todo.

Utilize a experiência realizada para aprimorar o próximo treinamento

Utilize as avaliações e a sua percepção para melhorar o próximo treinamento formal.

Conscientização não é só o grande evento

A realização de palestras ou outras formas de comunicação e de conscientização em s egurança da informação deve ser um grande evento, mas a conscientização em segurança da informação acontece cada dia, cada semana, ou no máximo a cada mês.

Periodicamente devem ser enviadas mensagens para os usuários sobre temas de segurança da informação, orientando-os e sempre que possível fazendo uma ligação com as políticas e normas de segurança de informação aprovadas e publicadas pela organização.

A maneira de se fazer esses pequenos eventos de conscientização pode ser das mais diversas maneiras. A criatividade não tem limite. Mas tenha sempre em foco que o objetivo não é fazer a mais criativa, mas sim, a comunicação mais adequada para os usuários.

Documento Política-Norma da Dimensão Conscientização e Treinamento do Usuário

O Documento Política-Norma da Dimensão Conscientização e Treinamento do Usuário em Segurança da Informação define os princípios básicos de como deve acontecer a conscientização e o treinamento do usuário.

Ele estabelece como a organização deseja que o evento de treinamento do usuário de segurança da informação aconteça, quem são os responsáveis, qual a periodicidade, tipos de grupos e outras regras gerais sobre o assunto.

Devem ser detalhados controles e regras que são comuns a todos os grupos de usuários. Caso existam situações especiais que exigirão um treinamento específico, poderão ser elaborados documentos mais detalhados para cada ambiente, tipo documento Padrão Nível 3, definido na Arquitetura de Política de Segurança da Informação, Item 2.2 – Arquitetura para a Política de Segurança da Informação, Aula 2. Porém, a Política-Norma da Dimensão Conscientização e Treinamento de Usuário em Segurança da Informação deve ser uma dimensão que terá menos subníveis de regulamentos.

Esse regulamento sobre Conscientização e Treinamento do usuário em Segurança da Informação considerar os seguintes elementos:

a. **Legislação ou Regras Corporativas**

Deve-se verificar se a organização está submetida a alguma legislação ou regra corporativa e neste caso é obrigada a adotar uma determinada forma e periodicidade de treinamento.

b. **Periodicidade do treinamento formal**

Deve-se definir qual deve ser a periodicidade do treinamento para os usuários.

c. **Responsabilidades pelo treinamento**

Deve-se definir quais são as áreas ou pessoas responsáveis pelo treinamento. Essa definição deve estar coerente com as definições de responsabilidade da área de Segurança da Informação.

É importante estar bem definida qual área estará custeando o treinamento. Evidentemente essa é uma questão bem específica da organização, mas muitas organizações não esclarecem essa questão e quando há a realização do treinamento, este acontece muito aquém do que a organização precisa e merece.

Exemplo prático de Política-Norma da Dimensão Conscientização e Treinamento do Usuário

Conscientização e Treinamento de Usuário em Segurança da Informação

1. **Objetivo deste regulamento**

Definir os requisitos e as regras para a existência de um processo de conscientização e treinamento do usuário em segurança da informação.

2. **Abrangência deste regulamento**

Este regulamento se aplica a todos os usuários que utilizam as informações do ambiente de tecnologia da organização.

Este regulamento está alinhado com o regulamento "Política de Segurança e Proteção da Informação."

3. **Implementação deste regulamento**

O Gabinete de Segurança da Informação, a Unidade de Segurança da Informação e as chefias das áreas da organização desenvolverão ações contínuas e necessárias para a implementação deste regulamento, ficando o Departamento de Segurança da Informação responsável pela coordenação dessas ações.

4. **Definições**

As definições de termos relativos à Segurança da Informação estão descritas no regulamento "Definições Utilizadas em Segurança da Informação".

5. **Política e regras**

5.1. Todo usuário de sistemas de informação da organização deve ser conscientizado e treinado em segurança da informação com o objetivo de garantir que o aspecto humano será fator positivo no processo de proteção da informação.

5.2. Esta conscientização e treinamento deverão ocorrer pelo menos uma vez por ano, de forma estruturada e registrada sua evidência para efeito de auditoria.

5.3. Antes de o usuário iniciar suas funções profissionais no acesso ao ambiente computacional, ele deve receber o treinamento de segurança da informação.

5.4. O usuário deve conhecer as políticas e normas de segurança da informação e deve assinar um termo de declaração de conhecimento desses regulamentos, bem como se comprometer a cumprir e zelar pelo cumprimento desses regulamentos.

5.5. Cada chefia é responsável por garantir que seus subordinados e prestadores de serviços terceirizados recebam o treinamento e a conscientização em segurança da informação.

5.6. Para exercer a função de Gestor da Informação, o usuário deverá fazer um treinamento específico sobre essa função dentro do processo de segurança.

5.7. Os profissionais de segurança da informação deverão buscar alcançar certificações profissionais internacionais aceitas pelo mercado, tipo CISM, CISA, CISSP ou CRISC.

5.8. As áreas de recursos humanos das diversas unidades organizacionais da organização deverão participar, e eventualmente coordenar, as atividades de conscientização e treinamento em segurança da informação.

5.9. A ação de conscientização e treinamento em segurança da informação é contínua e deve existir enquanto a organização existir.

6. **Conclusão**

O não cumprimento deste regulamento e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui falta grave e o usuário está sujeito à penalidades administrativas e/ou contratuais.

Situações de exceção e não previstas deverão ser definidas pelo Departamento de Segurança da Informação e pela Unidade de Segurança da Informação, considerando as áreas da organização envolvidas.

Exercício de fixação
Conscientização e treinamento do usuário

Identifique as políticas-normas existentes na sua organização e descreva se o que existe (situação atual) é suficiente para iniciar as atividades de conscientização e treinamento em segurança da informação para o usuário. Ou se seria necessário desenvolver alguns regulamentos, para existir o mínimo de regras, e somente depois começar o treinamento.

Quais são os regulamentos que você considera prioritários que existam antes do treinamento do usuário.

Considere a sua organização. Quais seriam os grupos (tipos) de usuários que você recomendaria que deveria existir para um treinamento de conscientização em segurança da informação. Justifique.

Considere a sua organização. Quais os tipos de treinamento que você indicaria para a sua organização durante os próximos cinco anos? De quem (ou de qual área) seria a responsabilidade para a gestão deste treinamento e quem (ou qual área) seria responsável pela operacionalização desse treinamento? Justifique e explique.

Sua organização possui Política-Normas da Dimensão de Conscientização e Treinamento de Usuário?

Se sim, explique o grau de efetividade desses regulamentos.

Se não, o que a falta desses regulamentos impactam no Processo Organizacional de Segurança da Informação?

Quais itens ou trechos do documento exemplo de Política-Norma Dimensão de Conscientização e Treinamento de Usuário você entende que precisam melhorar? Indique cinco. Justifique.

Quais itens ou trechos do documento exemplo Política-Norma Dimensão de Conscientização e Treinamento de Usuário que você entende que estão muito bons e você destacaria? Indique cinco. Justifique.

Considere a sua organização. Como você avalia a Dimensão de Políticas e Normas em relação às demais dimensões? Explique e justifique.

Conclusão – Política de Segurança da Informação

A política de segurança da informação é uma das Dimensões de Segurança e possui uma característica única: ela engloba todas as demais dimensões relacionadas à Segurança da Informação. O conjunto de regulamentos que definem a política de segurança da organização define como a organização deseja tratar cada uma das dimensões. Define como será o grau de rigidez dos controles de segurança da informação.

A Arquitetura da Política de Segurança da Informação apresentada neste treinamento é uma estrutura que facilita a ligação com cada uma das demais dimensões, permite uma graduação de granularidade dos controles, facilita a definição prática de quem deve assinar e validar cada regulamento. Essa arquitetura segue os temas tratados na família de Normas ISO/IEC 27000, com destaque para a Norma NBR ISO/IEC 27002.

Mais do que qualquer outra dimensão, essa dimensão somente será efetiva se os regulamentos que vão compor o conjunto da política de segurança da informação forem elaborados com a participação dos gestores da organização. O Gestor da Segurança da Informação tem a responsabilidade desenvolver esses regulamentos, mas esses regulamentos devem obrigatoriamente representar o que a organização deseja para a proteção da sua informação.

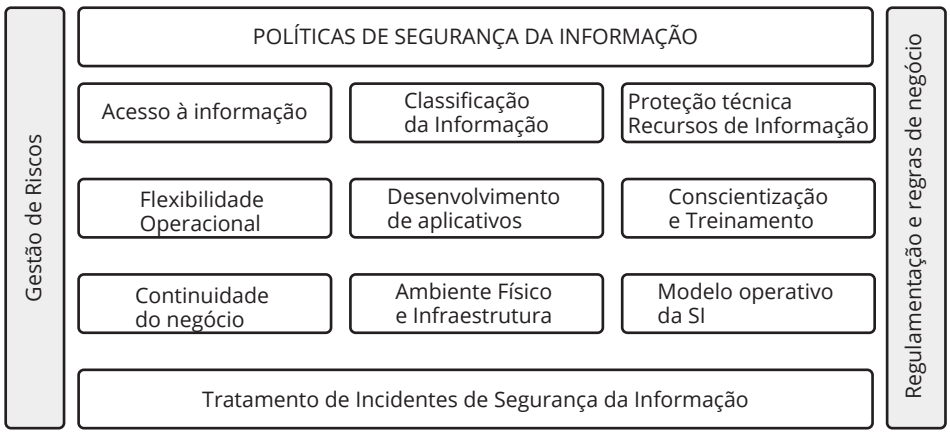


Figura 6.2
Segurança da informação e suas dimensões.

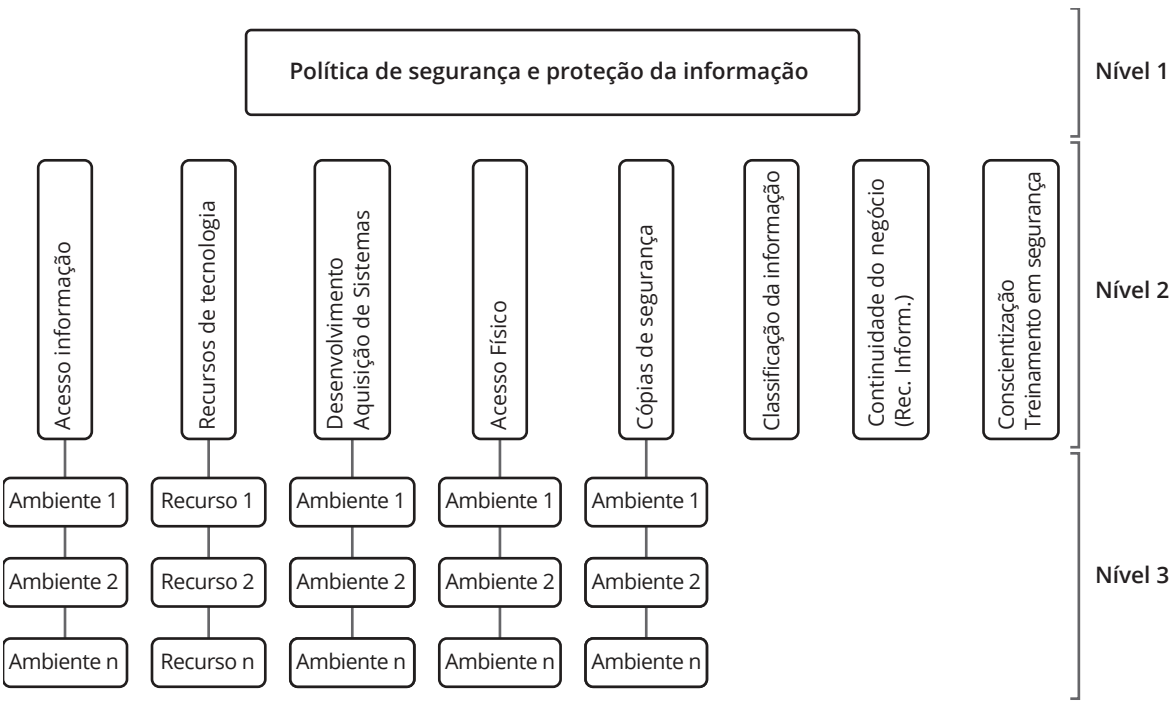
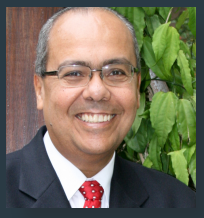


Figura 6.3
Estrutura da Arquitetura da Política de Segurança da Informação.

Bibliografia

- Livro: Praticando a Segurança da Informação - Edison Fontes
- Livro: Políticas e normas para a segurança da informação; Editora Brasport; Edison Fontes
- ISO 27001
- ISO 27002
- ISO 27005
- Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações. (Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1)
- Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. (Publicada no DOU Nº 125, de 03 Jul 2009 - Seção 1)



Edison Fontes é Mestre em Tecnologia pelo Centro Paula Souza do Governo do Estado de São Paulo; Bacharel em Informática pela UFPE, Certificado CISM, CISA e CRISC pela ISACA/USA, Professor em Cursos de Pós Graduação e Palestrante Corporativo. É autor de cinco livros sobre Segurança da Informação pelas Editoras Sicurezza, Saraiva e Brasport. Dedica-se ao assunto Segurança da Informação desde 1989. Desenvolveu Políticas de Segurança para várias Organizações, com destaque para o NOSI-Núcleo Operacional da Sociedade da Informação do Governo de Cabo Verde que foram transformadas em Lei. Exerceu a função de Security Officer em instituições financeiras (Banco BANORTE e RBS-Royal Bank of Scotland--Brasil) e em empresa de serviços de alta disponibilidade (GTECH Brasil). Atualmente desenvolve atividades como Consultor em Segurança da Informação.

esr.rnp.br

LIVRO DE APOIO AO CURSO

A partir das boas práticas do mercado e ainda da NC 03/IN01/DSIC/GSIPR, o curso de Políticas de Segurança da Informação desenvolve nos participantes habilidades e competências para que possam participar do processo de desenvolvimento e implementação de políticas de segurança nas suas organizações. Este curso abordará os conceitos e os padrões que devem ser seguidos para a organização desenvolver, implantar e manter a sua política de segurança da informação, como também, aplicar o conjunto das dimensões da segurança da informação como o elemento direcionador para a política de segurança da informação.

ISBN 978-85-63630-37-7