Unidade VIII

8 PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Como vimos, a informação é um dos bens mais valiosos de uma empresa, e para protegê-la são utilizados métodos e padrões que visam garantir confidencialidade, integridade e disponibilidade. Uma ferramenta importante é a política de segurança, que determina, de forma clara e simples, como a empresa pretende proteger suas informações. A política orienta a conduta das pessoas e serve de base para a criação de normas e procedimentos de segurança.

Antigamente, as informações das empresas ficavam centralizadas, e poucas pessoas (funcionários) as acessavam por meio de um computador – no caso, as que trabalhavam no CPD (centro de processamento de dados). Com o avanço tecnológico, as empresas começaram a disponibilizar computadores para todos os funcionários, de modo que as atividades fossem realizadas com maior rapidez e precisão. Em consequência, as informações deixaram de ser centralizadas, pois cada funcionário passou a ter acesso a elas de sua própria mesa. Com a descentralização, o controle ficou muito mais difícil. Daí a adoção de uma regulamentação interna, a política de segurança.

Um aspecto importante a considerar é a variedade cultural. O fato de as pessoas serem diferentes entre si, devido a culturas e percepções distintas, não é ruim. Dentro de uma empresa, porém, se cada funcionário tratar uma informação conforme sua percepção, as informações podem ficar vulneráveis. A política de segurança serve justamente para orientar a conduta de todos.

A política de segurança deve ser elaborada com base nas melhores práticas de mercado – por exemplo, ISO/IEC 27001 e 27002 (ABNT, 2005, 2006) –, na legislação nacional e internacional e na realidade da empresa. É importante publicar essa política em canais disponíveis para todos os funcionários, bem como realizar programas de conscientização em segurança da informação.

8.1 Política, normas e procedimentos de segurança da informação

O objetivo principal de uma política de segurança é ser um programa efetivo de proteção dos ativos de informação. A partir dela, podem-se estabelecer os procedimentos operacionais, as instruções de trabalho e os padrões de segurança.

Estudiosos do assunto dizem que, por trás de qualquer política de segurança, existem duas filosofias:

- **Filosofia proibitiva**: tudo o que não é expressamente permitido é proibido.
- **Filosofia permissiva**: tudo o que não é expressamente proibido é permitido.

Uma política de segurança não deve conter detalhes técnicos de mecanismos a serem utilizados; ela deve conter regras gerais, que se apliquem a toda a empresa. O detalhamento será especificado nas normas de segurança.

- **Política**: define o que fazer, em nível estratégico.
- **Normas**: definem o que fazer, em nível tático.
- **Procedimentos**: definem como fazer, em nível operacional.

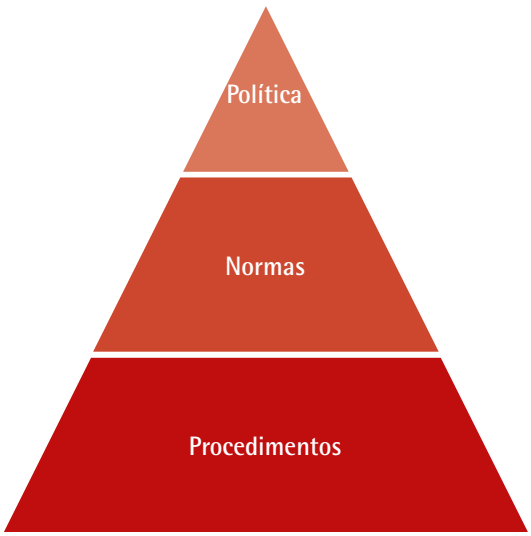

Figura 36 – Hierarquia entre política, normas e procedimentos

Os procedimentos são desdobramentos das normas, e estas são desdobramentos da política. Se há relação entre esses três elementos, a política é considerada alinhada.

Para o desenvolvimento de uma política de segurança, é necessário realizar uma análise de riscos que considere os seguintes aspectos:

- o que se deve proteger;
- as possíveis ameaças aos ativos de informação;
- o valor (a importância) de cada ativo de informação;
- o grau de proteção desejado pela empresa;
- os possíveis impactos no caso de perda de informações;
- o custo, o quanto a empresa está disposta a investir;
- a auditoria, a medição de quão efetiva está sendo a política.

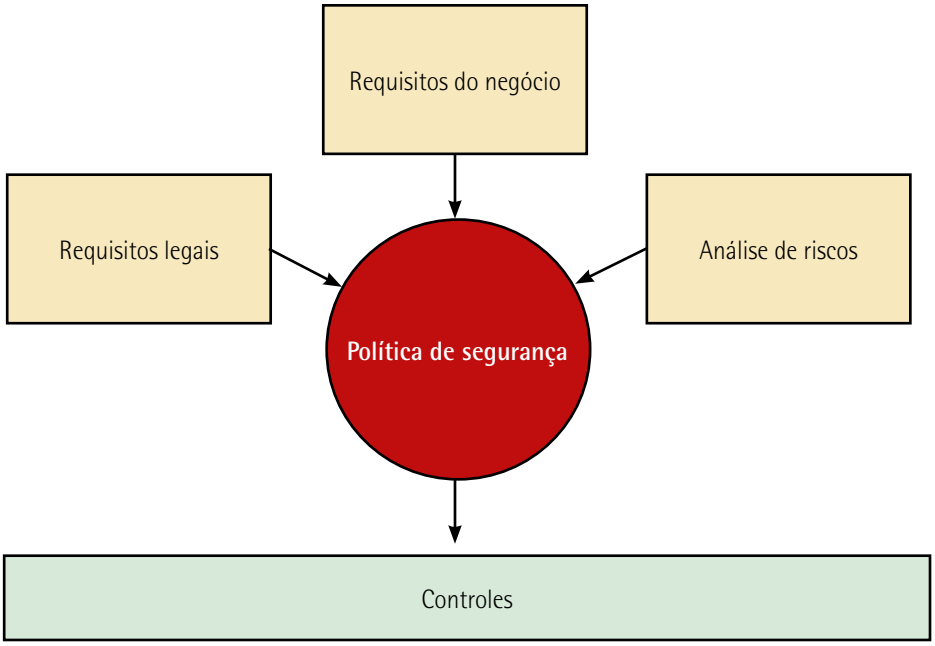

Figura 37 – Agentes que influenciam a criação de uma política de segurança

Uma política de segurança também deve prever:

- as sanções, caso não seja observada;
- as atualizações periódicas, com base no negócio da empresa e no avanço tecnológico;
- as responsabilidades dos envolvidos (executivos e funcionários da empresa).

Na criação da política de segurança, recomenda-se a participação de áreas específicas da empresa, a saber, a segurança da informação, a tecnologia, os recursos humanos, o jurídico e o comitê executivo de segurança da informação. Conforme o caso, outras áreas podem ser envolvidas.

As normas de segurança, como visto, estão um nível abaixo da política de segurança, a qual serve de base para sua criação. A seguir, apresentamos alguns exemplos de norma:

- **Classificação da informação**: normas para o tratamento e a rotulação das informações conforme seu nível de criticidade para a empresa.
- **Usuários de rede**: normas para o comportamento do usuário na rede da empresa. Por exemplo, procedimentos de criação, inclusão, alteração, manuseio, armazenamento e descarte de informações na rede, conexão de equipamentos, uso de senhas e bloqueio de estações de trabalho na ausência do funcionário.
- **Administradores de rede**: normas para os administradores de rede, baseadas nas regras estabelecidas para os usuários.

- **Uso de internet**: normas sobre o que o usuário pode fazer na internet concedida pela empresa.
- **Uso de e-mail**: normas sobre o que o usuário pode fazer no e-mail concedido pela empresa.
- **Uso de equipamentos portáteis**: normas sobre o que o usuário pode fazer com os equipamentos portáteis oferecidos pela empresa.
- **Redes sem fio**: normas para o uso correto das redes sem fio disponibilizadas pela empresa.
- **Acesso remoto**: normas sobre o que fazer em situações de acesso remoto externo e interno à rede da empresa.
- **Segurança lógica**: normas para impedir que usuários não autorizados se conectem ou obtenham acesso lógico aos sistemas e aplicações da empresa.
- **Segurança física**: normas para o acesso físico à empresa e para a circulação dentro dela.
- **Dispositivos de armazenamento**: normas para o uso de dispositivos de armazenamento (DVDs, CDs, pendrives etc.).
- **Mesa limpa**: normas sobre a organização da mesa trabalho, a fim de evitar que documentos confidenciais fiquem expostos.
- **Desenvolvimento de sistemas**: normas para a criação de qualquer sistema no ambiente da empresa. Devem ser aplicadas nas fases de produção, teste e validação do sistema.
- **Controle de acesso**: normas sobre as responsabilidades e os critérios para a concessão, a manutenção, a revisão e a revogação de acessos a sistemas de informação.
- **Certificação digital**: normas para a gestão de certificado digital dentro da empresa.
- **Manuseio e troca de dados**: normas para o manuseio e a troca de dados no âmbito da empresa.
- **Remanejamento e descarte de equipamentos**: normas para o usuário remanejar ou descartar um equipamento que não vai mais utilizar ou que será substituído.
- **Computação em nuvem**: normas para o uso da computação em nuvem, que atendam aos requisitos legais e aos anseios da organização.
- **Plano de continuidade de negócios**: normas para a continuidade de negócios em caso de interrupção inesperada do serviço.

Além das normas elencadas, outras podem ser desenvolvidas conforme a necessidade da empresa. O importante é que elas auxiliem o cumprimento da política de segurança nas mais diversas atividades da organização.

Convém que a política e as normas de segurança sejam acompanhadas da definição de termos específicos utilizados em sua composição. Em alguns casos, isso pode ser feito num documento à parte.

Lembrete

A política e as normas de segurança, mesmo que amparadas na legislação e nas melhores práticas, devem sempre refletir a cultura da organização.

As normas de segurança, assim como a política, descrevem as diretrizes para determinada atividade da empresa, o famoso **o que fazer**. O **como fazer** fica a cargo dos procedimentos.

Os procedimentos de segurança da informação são documentos que detalham como determinada diretriz da política ou das normas pode ser atendida pelo usuário. São também chamados de **documentos operacionais**.

Em alguns casos, para instruir o usuário a cumprir corretamente a política e as normas, as empresas adotam um documento específico, que pode ser uma cartilha, um manual ou até mesmo um termo de uso. Esse último desempenha duas funções: atribui ao usuário a responsabilidade por algum ativo de informação e indica a forma correta de usá-lo.

As normas podem determinar, por exemplo, que as estações de trabalho sejam bloqueadas automaticamente após cinco minutos de inatividade; os procedimentos vão orientar – no caso, o administrador da rede – sobre como fazer que isso ocorra tecnicamente (bloqueio automático).

É importante ter em mente que, na análise de riscos realizada para a elaboração da política, os procedimentos devem ser considerados, a fim de evitar que se crie uma diretriz que não possa ser cumprida.

8.1.1 Padrões de segurança da informação

Como indicado, a política, as normas e os procedimentos são elaborados de acordo com os padrões internacionais de melhores práticas em segurança da informação e as leis vigentes em cada país.

As melhores práticas de mercado são documentos criados por organizações internacionais e que servem como recomendações para a maioria das empresas. Elas não são obrigatórias, mas, devido ao uso em grande escala e à credibilidade conquistada, tornaram-se um requisito fundamental para as empresas demonstrarem sua preocupação com a segurança da informação.

Família 27000

A ISO (International Organization for Standardization) publicou várias normas relacionadas à segurança da informação, as quais atualmente são chamadas de **família 27000**.

As ISOs publicadas são validadas também pelo IEC (International Electrotechnical Commission) – daí a sigla ISO/IEC. No Brasil, a entidade oficial que traduz e disponibiliza essas normas é a ABNT

(Associação Brasileira de Normas Técnicas). Assim, as normas da ISO, quando usadas no Brasil, recebem a sigla ABNT NBR ISO/IEC.

Quadro 28 – Família 27000

Norma	Descrição
ISO 27000	Vocabulário de gestão da segurança da informação
ISO 27001	Requisitos para a implementação de um sistema de gestão
ISO 27002	Código de boas práticas para a gestão da segurança da informação
ISO 27003	Guia para a implementação do sistema de gestão da segurança da informação
ISO 27004	Métricas e meios de medição da eficácia de um sistema de gestão da segurança da informação
ISO 27005	Linhas de orientação para a gestão do risco da segurança da informação
ISO 27006	Requisitos e orientações para os organismos que prestam serviços de auditoria e certificação a um sistema de gestão da segurança da informação
ISO 27007	Critérios específicos para a auditoria dos processos do sistema de gestão da segurança da informação

Vale assinalar que as normas 27000 e 27006 ainda não foram publicadas, não havendo no momento previsão para que isso ocorra.

ISO 31000

Fornece princípios e diretrizes para a gestão de riscos. Atualmente, as empresas têm equipes que agem isoladamente, avaliando os riscos por meio de diversas ferramentas. Essa norma visa orientar as empresas para que desenvolvam, programem e melhorem continuamente a integração de tais áreas, o que traz benefícios para toda a organização.

ISO Guide 73

Apresenta a definição de termos genéricos relativos à gestão de riscos. Favorece a compreensão mútua e consistente, uma abordagem coerente na descrição das atividades relativas à gestão de riscos e a utilização de terminologia uniforme.

Cobit (Control Objectives for Information and Related Technology)

Guia de boas práticas apresentado como framework e dirigido para a gestão da tecnologia de informação. Muitos especialistas recomendam o Cobit para otimizar os investimentos de TI, e vários institutos realizam sua auditoria com ele.

Sarbanes-Oxley

A Sarbanes-Oxley é uma lei norte-americana criada em razão de escândalos financeiros corporativos. Seu objetivo é evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores por causa da aparente insegurança na governança das empresas. A lei orienta a elaboração de mecanismos de auditoria por meio de comitês. Estes podem supervisionar as operações da empresa, diminuindo os riscos

para o negócio e mitigando as fraudes. A transparência na gestão é indicada pela lei como ferramenta de credibilidade para a empresa. Muitas organizações do mundo que se relacionam com o mercado norte-americano comprometem-se a observar os princípios dessa lei.

Legislação e padrões brasileiros

Entre os dispositivos normativos nacionais, podemos destacar:

- Constituição Federal;
- Código Civil;
- Código Penal;
- Banco Central;
- Decreto nº 4.553/2002 – Classificação da Informação;
- Decreto nº 5.495/2005 – Política Nacional de Segurança da Informação;
- Lei nº 8.159/1991 – Política Nacional de Arquivos Públicos e Privados;
- Lei nº 9.279/1996 – Lei da Propriedade Intelectual;
- Lei nº 9.609/1996 – Lei do Software;
- Lei nº 9.610/1998 – Lei do Direito Autoral;
- Lei nº 105/2001 – Lei do Sigilo Bancário;
- Lei nº 12.965/2014 – Marco Civil da Internet;
- ABNT.

Observação

Dependendo da localização geográfica da empresa, devem ser observados tratados internacionais, leis territoriais e/ou leis estaduais e municipais.

8.2 Legislação e direito digital

O direito digital é uma evolução do próprio direito em face de um novo ambiente. As novas tecnologias, principalmente a internet, facilitam a geração, o compartilhamento e o armazenamento das informações, e essas atividades precisam ser regulamentadas.

Atualmente, o Brasil não tem uma legislação específica para regular as relações no mundo virtual; 95% dos problemas são solucionados com base na legislação vigente. Para as situações que as leis ainda não atendem, há projetos em andamento no Congresso Nacional.

Boa parte dos magistrados entende que a internet é apenas uma nova ferramenta para efetuar uma ação boa ou ruim. Todo ato praticado no mundo digital deixa um rastro, o que se pode chamar de **evidência** ou **prova**. Esse rastro produz efeitos jurídicos. Por exemplo:

- O fechamento de um contrato por meio de um simples **ok** numa mensagem de e-mail gera um compromisso entre as partes.

- Uma ofensa feita a uma pessoa ou a uma empresa por meio de um e-mail ou de uma postagem numa rede social obriga o autor da ofensa a uma reparação.

Em ambos os casos citados, o direito busca a satisfação das partes conforme os direitos ou deveres pleiteados, de maneira semelhante ao que acontece no mundo real. Cabe ressaltar que as novas tecnologias potencializaram determinadas situações ou ações, tanto no número de vezes que podem ocorrer quanto no efeito que podem causar.

A internet hoje é regulamentada da seguinte forma:

- No mundo:
  - ONU (Organização das Nações Unidas);
  - Uncitral (Comissão das Nações Unidas para o Direito Comercial Internacional);
  - Icann (Internet Corporation for Assigned Names and Numbers), instituição sem fins lucrativos, formada para assumir responsabilidades e estabelecer normas acerca de aspectos técnicos da internet, como endereços IP.

- No Brasil:
  - CGI (Comitê Gestor da Internet), criado pelo Decreto nº 4.829/2003.

Além de cumprir os acordos internacionais, para tratar de conflitos e delitos no mundo digital, o Brasil aplica suas próprias leis. Por exemplo: a Lei nº 12.965 (BRASIL, 2014), ou Marco Civil da Internet, regula o uso da internet no País. Sancionada em 23 de abril 2014 pela então presidente Dilma Rousseff, tentou sanar a ausência de uma lei específica.

Na internet, circulam muitas informações, disponíveis para usuários domésticos e corporativos. Assim como no ambiente físico, no ambiente digital pessoas mal-intencionadas podem se aproveitar das informações para cometer atos ilícitos.

Alguns usuários, às vezes até sem sabê-lo, infringem direitos alheios e cometem delitos. Há desavisados que acreditam ser a internet uma terra sem lei, o que não é verdade; há pessoas que pensam estar protegidas pelo anonimato no mundo digital, o que também não é verdade.

Fazer download de certos conteúdos (vídeo, imagem, texto, áudio) sem a devida autorização e enviar mensagens com vírus de computador ou com conteúdo ofensivo estão entre as ações que podem constituir um crime.

A maioria dos crimes cometidos pela internet ocorrem por falha humana. Mesmo com todas as ferramentas de segurança existentes, não há como prever as atitudes de quem está sentado diante do computador. Um usuário pode, por exemplo, ser enganado por uma mensagem de e-mail contendo um vírus. Mesmo desconhecendo o assunto e o remetente, ele clica na mensagem para visualizar o conteúdo dela, permitindo assim a instalação do vírus em sua máquina. Este, por sua vez, oculta-se no computador para poder coletar informações confidenciais – como senhas bancárias, números de cartão de crédito, CPF e RG – e enviá-las para uma máquina localizada em outra parte do mundo. De posse dessas informações, o golpista realiza fraudes na internet fazendo-se passar pela vítima.

A figura a seguir mostra um modelo do fluxo de um golpe internacional pela internet.

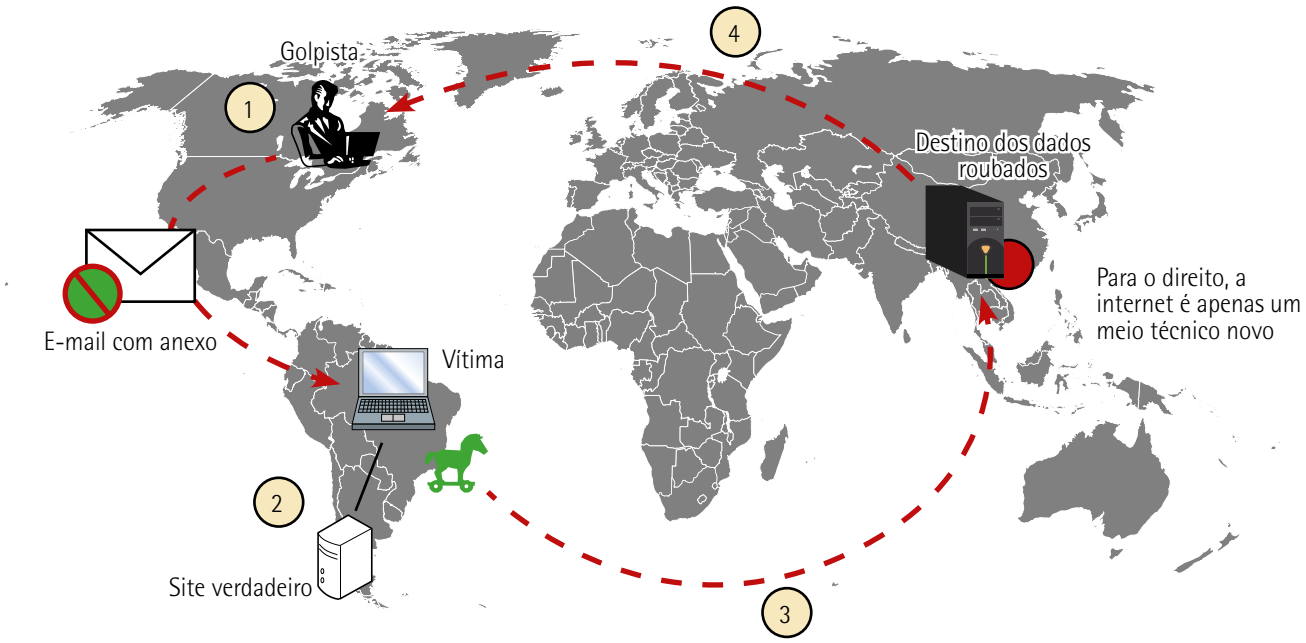

Figura 38 – Fluxo de um golpe internacional pela internet

Nesse cenário, torna-se cada vez mais necessária a cooperação entre os países para definir regras que permitam colher as evidências e levar os responsáveis à justiça.

O Marco Civil da Internet facilitou o relacionamento do Brasil com outros países. O País tem acordos firmados, por exemplo, com os Estados Unidos, a Alemanha, o Reino Unido e o Japão. Caso ocorra um

incidente envolvendo países que não assinaram um acordo, vai valer o bom relacionamento prévio entre eles, bem como os interesses comerciais de ambas as partes.

8.3 Time de resposta a incidentes computacionais

Diante das responsabilidades da área de segurança da informação no ambiente corporativo, a resposta a incidentes tem papel fundamental na eficácia do processo de gestão dos ativos de informação.

A maioria das instituições e empresas não utiliza uma única solução de segurança para combater todas as vulnerabilidades; em vez disso, estabelece camadas complementares de segurança, abrangendo tecnologia, processos e pessoas.

Uma das camadas adotadas para gerenciar o risco de segurança é o Cirt (computer incident response team, ou time de resposta a incidentes computacionais).

As principais motivações para criar um Cirt são:

- o crescente número de incidentes reportados;
- a promoção de políticas de segurança e procedimentos para melhorar o gerenciamento de riscos;
- as novas regulamentações e leis, que exigem controles de segurança sobre os sistemas de informação;
- o entendimento de que os administradores de rede não são capazes de proteger os recursos computacionais isoladamente.

Para estruturar um Cirt, é necessário compreender claramente o seu objetivo. Com esse intuito, vamos conceituar evento e incidente de segurança da informação.

Evento é uma ocorrência observável num sistema de informação. Por exemplo: um e-mail, um telefonema ou o travamento de um servidor (crash).

Incidente é um evento malicioso ou uma cadeia de eventos maliciosos num sistema de informação, que implicam o comprometimento ou a tentativa de comprometimento da segurança.

Exemplos de evento e incidente:

- Ataque de software malicioso:
  - **Evento**: um usuário informa que o computador dele pode ter sido contaminado por um vírus.
  - **Incidente potencial**: o sistema apresenta características típicas de contaminação por vírus.

- Ataque de DoS:
  - **Evento**: um usuário informa que não consegue acessar determinado serviço.
  - **Incidente potencial**: muitos usuários informam o mesmo problema.
- Invasão:
  - **Evento**: um administrador acredita que seu sistema foi invadido.
  - **Incidente potencial**: um administrador envia logs e trilhas de auditoria que indicam atividades suspeitas.
- Uso não autorizado:
  - **Evento**: um proxy mostra que um usuário tentou acessar um site pornográfico.
  - **Incidente potencial**: um proxy mostra que um usuário tentou acessar vários sites pornográficos

O Cirt é formado por um grupo de profissionais pertencentes a diversos departamentos da corporação, devidamente treinados e com larga experiência em suas respectivas áreas. Esse grupo tem a missão de atender e acompanhar, imediatamente, incidentes de segurança no ambiente computacional da empresa, segundo procedimentos previamente estabelecidos.

Embora a atuação do Cirt varie bastante, em razão da disponibilidade de pessoal, da capacitação da equipe, do orçamento etc., existem algumas recomendações de melhores práticas que se aplicam para a maioria dos casos:

- Obtenha o apoio da administração da empresa.
- Elabore um plano estratégico.
- Reúna informações significativas.
- Elabore e divulgue a missão do Cirt.
- Implemente o Cirt.
- Divulgue a entrada em operação do Cirt.
- Avalie continuamente a qualidade dos serviços prestados.

O apoio da administração da organização é fundamental, o que pode acontecer sob a forma de recursos (computadores, softwares etc.), financiamento, disponibilização de pessoal, tempo para o líder de segurança

criar o Cirt e espaço nos comitês de segurança para discutir o assunto. O apoio da administração da empresa também é importante porque dá respaldo às requisições do Cirt a outras áreas.

O pleno envolvimento dos participantes do Cirt e de seus superiores é um pré-requisito para a discussão posterior do orçamento necessário à implantação e à manutenção do time.

A elaboração de um plano estratégico deve levar em conta aspectos administrativos da concepção do Cirt. Algumas perguntas que podem ser feitas:

- Existem cronogramas a cumprir? Eles são realistas?
- Existe um grupo de projeto já formado?
- Como a organização toma conhecimento das ações de desenvolvimento do Cirt?
- Existe um membro que represente esse grupo numa instância superior?
- O processo está devidamente formalizado (e-mails, relatórios etc.)?
- Todos os membros do grupo estão a par das informações produzidas?

Reunir informações relevantes ajuda a definir as responsabilidades do Cirt e os serviços prestados por ele. Deve estar claro quais são as áreas e os sistemas mais críticos da empresa. Também é importante fazer um levantamento de eventos e incidentes reportados no passado, de modo que se dimensione o grau de conhecimento da empresa sobre eles. As informações reunidas ainda permitem descobrir se funcionários já existentes na empresa podem ser utilizados ou se há necessidade de novas contratações.

Alguns exemplos de informação relevante:

- último incidente com vírus na empresa;
- tentativas de invasão;
- fraudes envolvendo funcionários internos;
- funções do Cirt já cobertas por áreas existentes;
- procedimentos da empresa que contribuem para as funções do Cirt.

Agendar visitas em instituições similares e que já tenham um Cirt é um bom meio de obter mais informações.

Com base nos dados reunidos, elabore a missão do Cirt, que deve ser aprovada pela administração antes de sua divulgação à empresa. Precisa-se estar aberto para receber críticas e sugestões de melhoria da hierarquia.

Concluídas essas etapas, é hora de pôr o Cirt efetivamente em ação. Para isso:

- Contrate e treine o grupo principal do Cirt.
- Elabore a metodologia de trabalho e divulgue-a entre todos.
- Compre e instale os equipamentos e softwares de suporte ao Cirt.
- Defina as especificações de recuperação de evidências de incidente para cada sistema crítico.
- Desenvolva modelos de relatório e mecanismos de informação de incidentes.

Quando o Cirt estiver operacional, elabore uma campanha de divulgação que informe aos colaboradores as funções do grupo, os funcionários envolvidos e as formas de entrar em contato para reportar incidentes. Esse procedimento precisa ser repetido de tempos em tempos.

A avaliação periódica do Cirt deve considerar as estatísticas de incidentes reportados, os incidentes resolvidos, os falsos positivos e o tempo de indisponibilidade de sistemas. A comparação com outras empresas também é necessária. A correta manutenção e o aumento da base de conhecimento documentado ajudam no aprimoramento dos membros do Cirt.

O Cirt é formado por profissionais de diferentes áreas para atender à necessidade de, em face de um incidente, atuar em várias frentes ao mesmo tempo, identificando as causas e coletando as evidências do ataque. Esses funcionários não se dedicam apenas ao Cirt. No entanto, quando acionados pelo líder do Cirt, têm de responder imediatamente.

O líder do Cirt deve ser um funcionário com ampla experiência em segurança da informação e em gerenciamento de projetos de tecnologia. Recomenda-se que ele tenha um cargo na hierarquia que possibilite a tomada de decisões, a requisição de auxílio a funcionários de outras áreas e a condução de verificações nas diversas áreas da corporação. Esse líder pode ser um gerente ou um diretor da área de segurança da informação.

A área de segurança da informação deve instruir os funcionários das outras áreas a identificar, coletar e/ou preservar os rastros do incidente. Também cabe a ela avaliar as consequências de um ataque e, se necessário, providenciar a execução do plano de continuidade de negócios. Ao fim do acompanhamento de um incidente, deve coordenar a elaboração do relatório, descrevendo o(s) fato(s) ocorrido(s).

A área de redes deve prover o acesso a equipamentos de comunicação e segurança sob sua responsabilidade, como firewalls, roteadores e switches, sempre que requisitado pelo líder do Cirt, a fim de auxiliar o levantamento e a análise dos logs. Quando for preciso, deverá entrar em contato com provedores de acesso, empresas de telecomunicações etc.

A área de manutenção de servidores deve averiguar detalhadamente a configuração dos servidores, em virtude de possíveis acessos não autorizados, e coletar o rastro de transações por meio da verificação

do código das aplicações. O líder do Cirt pode requisitar que determinado servidor (ou um conjunto deles) seja mantido em quarentena para uma apuração mais precisa. Nesse caso, compete à equipe designada providenciar a instalação e a configuração de servidores sobressalentes para assumir o ambiente de produção.

A área de auditoria deve identificar quais controles de segurança ou procedimentos falharam e permitiram a ocorrência do incidente. Sua missão é auxiliar o líder do Cirt na elaboração do relatório do incidente e validar/auditar a implementação do plano de ação preparado para solucioná-lo. A auditoria também contribui com o Cirt na estimativa dos prejuízos financeiros e de imagem causados pelo incidente.

A área de inspetoria deve colaborar para a identificação das causas e motivações do incidente. É igualmente de sua responsabilidade a manutenção do histórico de todos os incidentes identificados ou reportados na corporação, subsidiando o líder do Cirt com informações sobre padrões de comportamento, objetivos, frequência e medidas adotadas em casos semelhantes.

A área de recursos humanos é acionada quando um incidente envolve funcionários ou terceiros que prestam serviços para a instituição. O líder do Cirt, nesse caso, requisita informações sobre o(s) funcionário(s) envolvido(s), como formação, cargo e responsabilidades.

A área jurídica é acionada para oferecer auxílio jurídico na coleta e preservação de evidências e no tratamento com empresas parceiras, clientes ou funcionários envolvidos. Toda a comunicação entre as partes deve ser acompanhada pela área jurídica da organização.

A área de relações públicas é acionada no caso de o incidente provocar a exposição da empresa diante do público. Essa área orienta a comunicação com os clientes, os parceiros e a imprensa (se necessário).

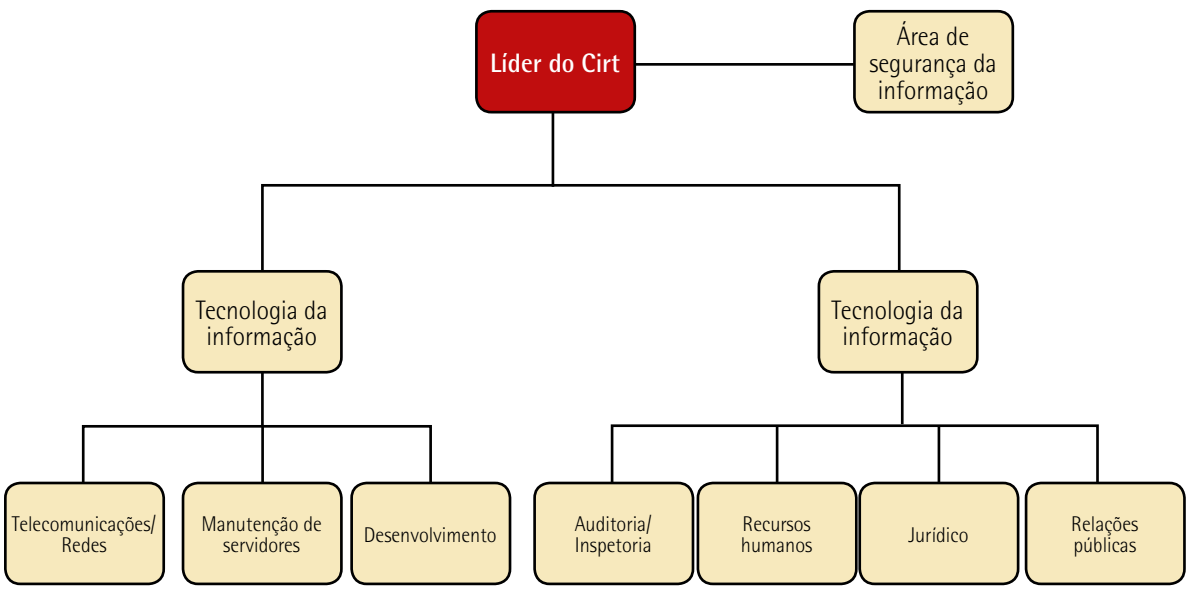

Figura 39 – Organograma do Cirt

O fluxo de resposta a incidentes deve seguir esta sequência lógica:

- Sempre que um incidente for informado ou detectado, ele deverá ser encaminhado ao responsável pela área de segurança da informação.
- Em função da gravidade do incidente, a segurança da informação decidirá se o Cirt vai ser acionado ou não.
- Sendo acionado, o Cirt deverá abrir um chamado de incidente.
- Esse chamado é composto de um relatório, o qual precisará ser preenchido durante todo o acompanhamento do incidente.

Ao fim do trabalho, ou mesmo durante sua execução, o líder do Cirt apresentará ao comitê de segurança um resumo do relatório, que deverá conter:

- uma descrição sucinta do incidente;
- a causa do incidente;
- a forma de identificação do incidente;
- a indicação quanto a se pode haver consequências financeiras e de imagem;
- as contramedidas tomadas;
- o plano de ação para a contenção de incidentes semelhantes.

O acionamento do Cirt deve ser feito por canais de fácil acesso, como um ramal telefônico exclusivo, um endereço de e-mail genérico (cirt@empresa.com.br) ou uma página de webmail na intranet (para não identificar o emissor).

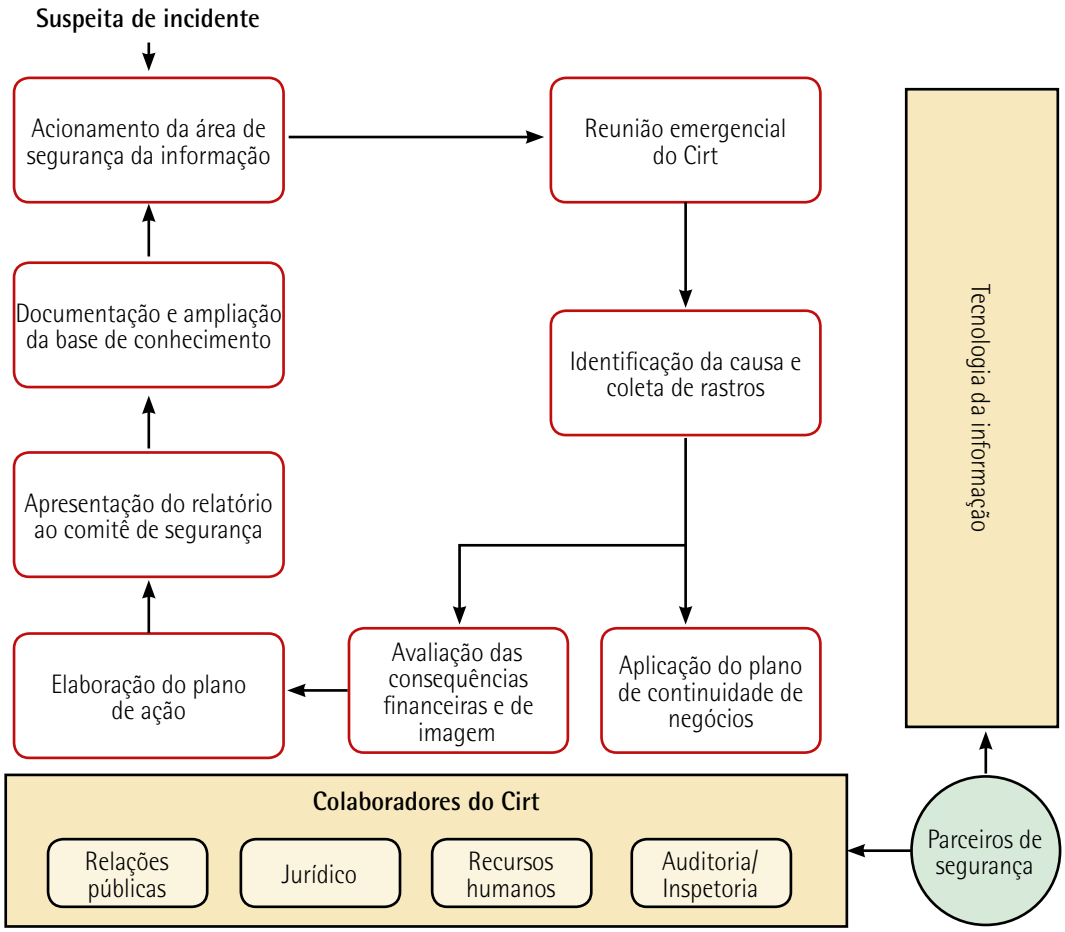

Figura 40 – Fluxo da gestão de incidentes

8.4 Plano de continuidade de negócios

Uma organização pode estar sujeita a diversos incidentes, os quais têm potencial de causar prejuízos ainda não previstos ou ainda não imagináveis. Essas peculiaridades necessitam de tratamento diferenciado, sempre visando proteger os ativos de informação.

Vejamos como funciona um plano de continuidade de negócios, detalhando seu conceito e as metodologias para implantá-lo.

> Um BCP (business continuity plan) ou PCN (plano de continuidade de negócios) tem em sua essência diversos procedimentos e medidas, cujo objetivo é minimizar as perdas decorrentes de um possível desastre. Entende-se por desastre a ocorrência de um evento súbito, de grande magnitude, que possa causar grandes prejuízos aos ativos e processos (RAMOS, 2008, p. 154).

Exemplos de desastre são enchentes, incêndios ou grandes manifestações.

O PCN pode ser considerado uma evolução do DRP (disaster recovery plan) ou PRD (plano de recuperação de desastres). Este considerava somente os ativos de tecnologia da informação. O PCN, por sua vez, além da área de TI, engloba pessoas e processos. A criação e a manutenção desse plano integram a chamada **gestão de continuidade de negócios**.

O que define a implantação de um PCN é o tempo máximo de parada num processo crítico da organização. Se a empresa tiver um processo que não possa ficar parado por um período superior a 48 horas, na elaboração do PCN serão considerados todos os recursos necessários para o funcionamento dele (instalações físicas, sistemas de TI, colaboradores e fornecedores).

A primeira etapa da implantação de um PCN é o entendimento do negócio, que deve ser feito sob a ótica da continuidade de processos, identificando-se os aspectos críticos a serem preservados. Também se devem levar em conta os argumentos que serão usados para justificar a execução do plano. Hoje existem no mercado diversas ferramentas que auxiliam o gestor a realizar essa tarefa.

Saiba mais

Para conhecer mais sobre metodologias de execução do plano, acesse o site do DRII (Disaster Recovery Institute International):

<www.drii.org>.

Ainda nessa primeira etapa, a escolha da equipe que vai participar do PCN é essencial. O coordenador do projeto deve ter amplo conhecimento da empresa, bem como acesso à alta direção e a outras áreas da empresa.

O próximo passo é a execução do BIA (business impact analysis) ou AIN (análise de impacto nos negócios), que visa avaliar quais impactos a ocorrência de um incidente ou de um desastre terá na organização, bem como analisar o tempo máximo permitido de parada. Nesse momento, não é necessário preocupar-se com a probabilidade de o evento acontecer, e sim com o efeito que ele pode ter se acontecer.

Para esse levantamento, é importante consultar os gestores dos processos – ninguém melhor do que eles para identificar a criticidade dos processos. Devem-se considerar também os aspectos financeiros, operacionais, legais e regulatórios.

A etapa seguinte é a definição estratégica de como garantir a disponibilidade de recursos, metodologias e processos, permitindo assim a continuidade dos processos críticos em caso de desastre.

De acordo com Ramos (2008), existem três modelos de estratégia:

- **Ativo/backup**: uso de recursos sobressalentes, que podem ser acionados em caso de desastre.

- **Ativo/ativo**: uso de duas ou mais localidades operacionais separadas geograficamente, dividindo as operações, sendo uma a contingência da outra.

- **Localidade alternativa**: modelo intermediário entre os outros dois apresentados; uma localidade recebe parte das operações de forma periódica, para homologar seu funcionamento.

Outro passo importante é o estabelecimento de um PAC (programa de administração de crises), que define as ações a tomar diante da ocorrência de um desastre, inclusive o contato com agentes externos, como defesa civil e imprensa.

Algo que se deve ter em mente é que o PCN necessita de atualização constante, a fim de se adequar à realidade da organização. Esse processo só é possível por meio de um modelo de gestão preocupado com a manutenção do plano.

A falta de determinada cultura nas organizações é uma parte importante a ser trabalhada no desenvolvimento e na implementação de planos de continuidade. Os colaboradores precisam estar cientes do uso correto dos recursos da empresa, bem como da necessidade de continuidade dos processos críticos.

Na figura a seguir, vemos um esquema dos passos para implantar a gestão de continuidade de negócios.

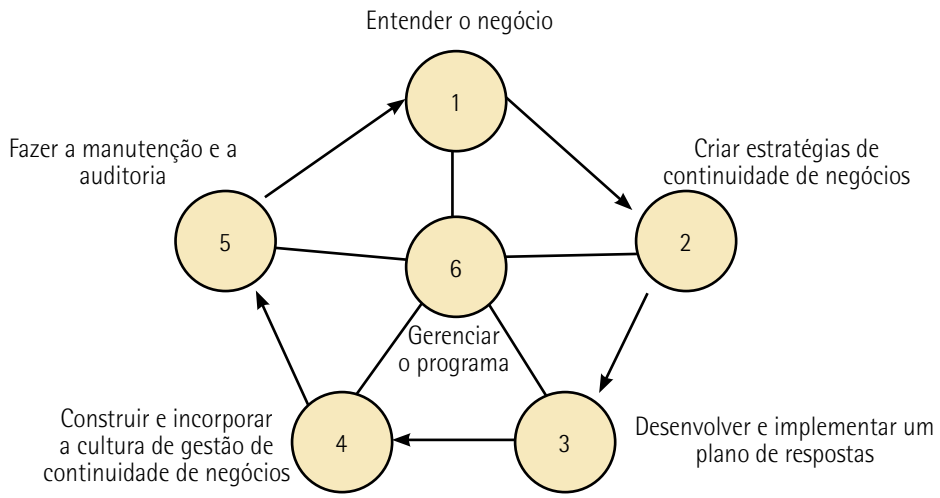

Figura 41 – Gestão de continuidade de negócios

A melhor forma de definir os procedimentos a adotar em caso de incidente é a execução de testes. Nenhum plano pode ser considerado maduro se não forem realizadas simulações.

As pessoas envolvidas devem conhecer os procedimentos antes que seja necessário empregá-los. Não teria sentido elas pararem todo o processo para ler um manual de instruções sobre o que fazer.

Um processo de revisão garante a melhoria contínua dos procedimentos estabelecidos, e um processo de auditoria independente contribui para a maturidade do plano, aumentando a confiança no trabalho feito.

As estratégias de recuperação têm por objetivo garantir a continuidade dos processos críticos, previamente mapeados, atendendo ao TMP (tempo médio de parada) estabelecido.

Para escolher as estratégias, é preciso ter em mente os custos diretos e indiretos e avaliar o pior cenário possível diante de um desastre. Alguns elementos a considerar:

- **Usuários:** a parte mais importante de um PCN. Deve-se garantir que, em caso de desastre, as atividades deles não sejam interrompidas. Para isso, é necessário cuidar de aspectos como integridade física, ambiente de trabalho e disponibilidade de informações médicas.

- **Logística**: fator de grande impacto nas entregas de uma empresa, mesmo quando o desastre não afeta diretamente a organização. Podem-se citar como exemplo as greves de correios e caminhoneiros e os gargalos de transporte por falta de infraestrutura.

- **Instalações**: deve-se estar atento aos serviços básicos (como água, energia elétrica, ar-condicionado e gás), ao espaço físico e a toda a infraestrutura de comunicação.

- **Dados**: o armazenamento de informações é um ponto bastante crítico. Para garantir a disponibilidade delas em caso de desastre, diversas tecnologias podem ser usadas, como backup e transferência remota de informações.

Dependendo da criticidade do processo e do orçamento da empresa para a estratégia de recuperação, alguns tipos de site podem ser utilizados:

- **Cold site**: local físico, sem nenhuma instalação básica de comunicação ou energia, que pode receber os equipamentos. É a opção mais barata, mas leva muito tempo para entrar em funcionamento caso ocorra um desastre.

- **Warm site**: junção de um cold site com os serviços básicos de infraestrutura, como instalação elétrica, links de comunicação e cabeamento interno de rede. Alguns podem conter até computadores. Esse modelo, porém, não contempla servidores, mainframes etc. Tais equipamentos são disponibilizados somente na ocorrência de um desastre.

- **Hot site**: espaço semelhante ao ambiente de produção em termos de infraestrutura, à espera apenas da ocorrência de um incidente para entrar em funcionamento. Entretanto, as informações nele não estão sincronizadas, sendo necessário o envio dos dados para o seu funcionamento completo.

- **Mirror site**: similar ao hot site, mas com sincronismo das informações. É a estratégia que oferece o tempo de resposta mais rápido, embora seja também a de maior custo.

A figura a seguir mostra a relação do tempo necessário para a ativação do site com o investimento em sua construção.

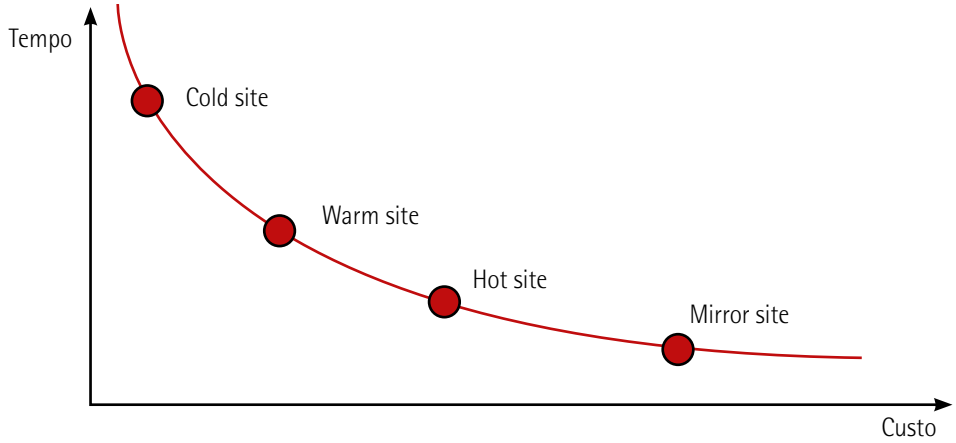

Figura 42 – Relação entre tempo e custo das estratégias de recuperação

Resumo

Nesta unidade, vimos os processos de segurança da informação, que ganharam uma importância fundamental na redução dos riscos. Tratamos de políticas, normas e procedimentos de proteção alinhados ao negócio, que regulam internamente a segurança da informação. Essas regras devem ser conhecidas e cumpridas por todos na empresa.

Consideramos depois a legislação e o direito digital. Assinalamos que, no Brasil, não existe uma legislação específica para regular as relações no mundo virtual, e que 95% dos problemas são solucionados com base na legislação vigente. Isso porque boa parte dos magistrados entende que a internet é apenas uma nova ferramenta para efetuar uma ação boa ou ruim.

Por último, mostramos que, quando todos os procedimentos adotados não são suficientes, deve-se acionar um plano B, a saber, o time de resposta a incidentes computacionais e o plano de continuidade de negócios, um para responder de forma organizada às tentativas de invasão, o outro para entrar em ação caso a falta de algum serviço (água, luz etc.) comprometa a disponibilidade das informações.

FIGURAS E ILUSTRAÇÕES

Figura 3

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *Guide 51*: safety aspects: guidelines for their inclusion in standards. Geneva, 2014. p. 7. Adaptada. Disponível em: <http://isotc.iso.org/livelink/livelink/open/8389248>. Acesso em: 5 jul. 2018.

Figura 4

640PX-TOKEN_VERISIGN.JPG. Disponível em: <https://upload.wikimedia.org/wikipedia/commons/thumb/3/3d/Token_Verisign.JPG/640px-Token_Verisign.JPG>. Acesso em: 5 jul. 2018

Figura 5

640PX-MOSCOW_TROLLEYBUS_TICKET_VALIDATE_(37919052671).JPG. Disponível em: <https://upload.wikimedia.org/wikipedia/commons/thumb/3/33/Moscow_trolleybus_ticket_validate_%2837919052671%29.jpg/640px-Moscow_trolleybus_ticket_validate_(2837919052671)29.jpg>. Acesso em: 5 jul. 2018.

Figura 6

Grupo UNIP-Objetivo.

Figura 7

Grupo UNIP-Objetivo.

Figura 17

MORAES, A. F. *Segurança em redes*: fundamentos. São Paulo: Érica, 2010. p. 172.

Figura 20

MORAES, A. F. *Segurança em redes*: fundamentos. São Paulo: Érica, 2010. p. 167. Adaptada.

REFERÊNCIAS

Audiovisuais

O JOGO da imitação. Dir. Morten Tyldum. Reino Unido: Black Bear Pictures; Bristol Automotive, 2014. 114 minutos.

Textuais

ARIMA, C. H. *Metodologia de auditoria de sistemas*. São Paulo: Érica, 1994.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *NBR ISO/IEC 27001*: tecnologia da informação: técnicas de segurança: sistemas de gestão de segurança da informação: requisitos. Rio de Janeiro, 2006.

___. *NBR ISO/IEC 27002*: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BEAL, A. *Segurança da informação*: princípios e melhores práticas para proteção de ativos de informação nas organizações. São Paulo: Atlas, 2005.

BRADLEY, S. 4 passos para não ter problemas de segurança com redes VPN. *ComputerWorld*, 27 jun. 2018. Disponível em: <http://computerworld.com.br/4-passos-para-nao-ter-problemas-de-seguranca-com-redes-vpn>. Acesso em: 5 jul. 2018.

BRASIL. Instituto Nacional de Tecnologia da Informação. *ICP-Brasil*. Brasília, 2017. Disponível em: <http://www.iti.gov.br/icp-brasil>. Acesso em: 5 jul. 2018.

___. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 5 jul. 2018.

___. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Medida provisória n° 2.200-2, de 24 de agosto de 2001*. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 5 jul. 2018.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.BR). *Cartilha de segurança para internet*. São Paulo, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 5 jul. 2018.

FLORENZANO, C. Mapa mostra em tempo real regiões afetadas por mega-ataque de ransomware. *CBSI*, 12 maio 2017. Disponível em: <https://www.cbsi.net.br/2017/05/mapa-mostra-em-tempo-real-regioes-afetadas-por-mega-ataque-ransomware.html>. Acesso em: 5 jul. 2018.

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. Tradução Ariovaldo Griesi. 4. ed. São Paulo: McGraw Hill, 2008

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). *Guide 51*: safety aspects: guidelines for their inclusion in standards. Geneva, 2014. Disponível em: <http://isotc.iso.org/livelink/livelink/open/8389248>. Acesso em: 5 jul. 2018.

MCGEE, B. O WPA2 está quebrado. E aí? *CIO*, 18 out. 2017. Disponível em: <http://cio.com.br/opiniao/2017/10/18/o-wpa2-esta-quebrado-e-agora/>. Acesso em: 5 jul. 2018.

MITINIK, K.; SIMON, W. L. *A arte de enganar*: ataques de hackers: controlando o fator humano na segurança da informação. Tradução Kátia Aparecida Roque. São Paulo: Pearson, 2003.

MORAES, A. F. *Segurança em redes*: fundamentos. São Paulo: Érica, 2010.

NEWMAN, O. *Defensible space*: crime prevention through urban design. New York: MacMillan, 1972.

RAMOS, A. *Security officer 2*: guia oficial para formação de gestores em segurança da informação. Porto Alegre: Zouk, 2008.

RIBEIRO, G. WPA3 deve chegar ainda em 2018 para tornar conexão Wi-Fi mais segura. *TechTudo*, 10 jan. 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/01/wpa3-deve-chegar-ainda-em-2018-para-tornar-conexao-wi-fi-mais-segura.ghtml>. Acesso em: 5 jul. 2018.

THE PENETRATION testing execution standard. 2014. Disponível em: <http://www.pentest-standard.org/index.php/Main_Page>. Acesso em: 5 jul. 2018.

WEIDMAN, G. *Testes de invasão*: uma introdução prática ao hacking. São Paulo: Novatec, 2014.

Sites

<http://cve.mitre.org/>.

<http://www.cert.br/>.

<http://www.cert.org/>.

<http://www.drii.org/>.

<http://www.rfc-editor.org>.

Interativa

Informações:
www.sepi.unip.br ou 0800 010 9000