XPe

Aprenda com quem faz

Fundamentos em Segurança Cibernética Defensiva

Mário Luiz Moura Júnior

2022

SUMÁRIO

Capítulo 1. Conceitos Básicos 5

Introdução 5

Pilares da Segurança da Informação 7

Ativo, Vulnerabilidade, Ameaça, Impacto e Risco 8

Indicadores 8

PDCA 10

NOT – Network Operations Center 11

SOC – Security Operations Center 11

CSIRT 13

Capítulo 2. Governança Corporativa 16

Valores da Governança 18

Governança Corporativa Aplicada em TI 19

COBIT 20

ITIL 22

PMBOK 24

Capítulo 3. ISO27000 27

Sistema de Gestão da Segurança da Informação (SGSI) 27

ISO27005 29

Capítulo 4. Governança de Dados 32

Proteção e Privacidade de Dados e Dados Pessoais 32

Princípios da Governança de Dados 34

Capítulo 5. Direito Digital 38

LGPD – Lei Geral de Proteção de Dados 40

Capítulo 6. Crimes Virtuais 44

Principais tipos 44

Como se proteger 46
Capítulo 7. Entidades de Apoio 49
Capítulo 8. Tratamento de Incidentes 51
Referências 54

> Capítulo 1

Capítulo 1. Conceitos Básicos

Introdução

A segurança da informação é a área de conhecimento que agrega um conjunto de habilidades, recursos, processos e ferramentas necessárias para garantir a confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade das informações de uma organização ou indivíduo.

A defesa cibernética tem por objetivo evitar que possíveis ataques cibernéticos tenham sucesso em um ambiente computacional. Ela contempla a prevenção, monitoramento e execução de contramedidas para antecipar, interromper e responder eventuais atacantes.

Considerando-se as perspectivas econômicas vigentes, as empresas vêm buscando o aumento da sua eficiência operacional limitando investimentos e reduzindo custos. Esse é um cenário particularmente desafiador para a segurança da informação, considerando que:

- O relatório *VERIZON, 2020 Data Breach Investigation Report* mostra que o tempo para uma falha de segurança ser explorada numa empresa tem ordem de grandeza de minutos. Por outro lado, o tempo para solução está na ordem de dias.
- Existem diversas ferramentas disponíveis on-line para a realização de ataques, mesmo por pessoas sem grande domínio técnico.
- As técnicas para a realização de ataques evoluem mais rápido que as técnicas de prevenção, deixando as empresas expostas.
- A proliferação de dispositivos, fabricantes e tecnologias conectadas à Internet, trafegando conjuntamente dados corporativos e

pessoais, tem sido grande. BYOD e IOT são exemplos da complexidade e do potencial risco para o ambiente.

- A adoção da nuvem também se mostra um grande desafio para as empresas. Os dados e serviços estão espalhados pela Internet eventualmente, com provedores despreparados para lidarem com questões de segurança.

- Os requisitos legais de segurança de diversos setores estão cada vez mais restritos e específicos. As empresas com ações em bolsa e seus fornecedores, por exemplo, precisam atender a uma série de requisitos para reduzirem os riscos para os seus acionistas.

- A adoção massiva das redes sociais abrindo oportunidade para o uso intensivo da engenharia social.

O desenvolvimento e a implantação da defesa cibernética nas empresas tornam-se cada vez mais necessários. Caso uma invasão ocorra, deve-se responder o quanto antes às seguintes perguntas:

- Como (*How*) podemos detectar uma invasão?

- Por que a invasão ocorreu (*Why*)?

- Qual (*What*) é o impacto no negócio?

- Quem (*Who*) é responsável por detectar e reagir à invasão?

- Quem (*Who*) deve ser informado ou envolvido e quando (*When*), para que uma decisão seja tomada?

Quem (*Who*) e quando (*When*) deve-se, interna ou externamente, avisar sobre a invasão?

Pilares da Segurança da Informação

Os conceitos abaixo são a base da defesa cibernética. O comprometimento de um ou mais destes elementos pode colocar em risco a sobrevivência da sua organização. Todas as atividades da área devem reduzir as chances de um ou mais pilares serem quebrados. Questione-se:

"Esta atividade de rotina ou este projeto reduz a exposição da minha organização?". Se a resposta for não, é hora de repensar o que faz no seu dia a dia. Foco é essencial.

- Confidencialidade (*Confidentiality*): garantir que a informação foi disponibilizada apenas para as pessoas autorizadas.
- Integridade (*Integrity*): é garantir a precisão, consistência e confiabilidade dos dados durante todo o seu ciclo de vida, impedindo atualizações não autorizadas.
- Disponibilidade (*Availability*): garantir que a informação está disponível para as pessoas autorizadas, conforme os padrões acordados.

Os termos acima são conhecidos como Tríade CIA (*Confidentiality, Integrity e Availability*). Alguns novos termos foram acrescidos à tríade, sendo considerados também essenciais no nosso dia a dia:

- Autenticidade: garantir que a mensagem, transação ou troca de informações venha da fonte que afirma ser.
- Irretratabilidade (não repúdio): garantir que ninguém possa negar a validade de algo.

Conformidade: garantir que as leis, regras e procedimentos necessários para garantir os princípios acima sejam devidamente implantados e executados.

Ativo, Vulnerabilidade, Ameaça, Impacto e Risco

Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você conhece a si mesmo, mas não conhece o inimigo, para cada vitória ganha, sofrerá também uma derrota. Se você não conhece nem o inimigo e nem a si mesmo, perderá todas as batalhas. (TZU. A Arte da Guerra, 2006).

- Ativo: um elemento qualquer (informação, software, hardware, pessoa por exemplo) que agregue valor ao negócio e que ao ter a sua confidencialidade, integridade ou disponibilidade, poderá comprometer a organização ou indivíduo. O ativo deverá ser adequadamente monitorado ou protegido.

- Vulnerabilidade: uma fraqueza que pode ser explorada por uma ou mais ameaças.

- Ameaça: um evento ou circunstância com potencial para impactar negativamente o ambiente de TI.

- Impacto: a exposição de um dos princípios listados anteriormente a partir da exploração de uma vulnerabilidade por uma ameaça.

- Risco: probabilidade de exposição ou perda resultante de uma vulnerabilidade sendo explorada por uma ameaça.

Indicadores

"Não se gerencia o que não se mede,
não se mede o que não se define,
não se define o que não se entende,
e não há sucesso no que não se gerencia."

- William Edwards Deming, 1989.

- Qual incidente de segurança devemos priorizar?

- Quantas falhas de segurança tivemos no último mês?
- Qual o impacto financeiro tivemos na última invasão?
- Qual vulnerabilidade devemos mitigar primeiro?

As perguntas acima não podem ser respondidas com “acho”. Um conjunto de indicadores robusto é a base da segurança da informação.

A definição de um conjunto mínimo de indicadores para cada serviço ou processo é fundamental para o monitoramento da qualidade das entregas oferecidas. Para isso, é necessário identificar:

- Fator Crítico de Sucesso (FCS): situação que deve acontecer para que seja considerado que um serviço foi realizado com sucesso.
- Key Performance Indicator (KPI): indicador usado para medir a realização de cada FCS. Deve-se considerar de 3 a 4 KPIs para cada FCS. Sempre que um KPI for ofendido, será necessário elaborar um plano de ação para restaurar os níveis de serviço aos valores adequados.
- Indicadores operacionais: outros indicadores que auxiliam na gestão da qualidade do serviço. Esses indicadores auxiliam na identificação de possíveis desvios antes que os KPIs sejam afetados.

Um indicador (KPI ou operacional) pode ser classificado entre uma das quatro dimensões abaixo. Deve-se, dentro do possível, abordar todas as dimensões no gerenciamento de um serviço ou processo.

- Aderência: verifica a adoção aos processos estabelecidos.
- Eficiência: verifica a alocação de recursos para a execução do serviço.

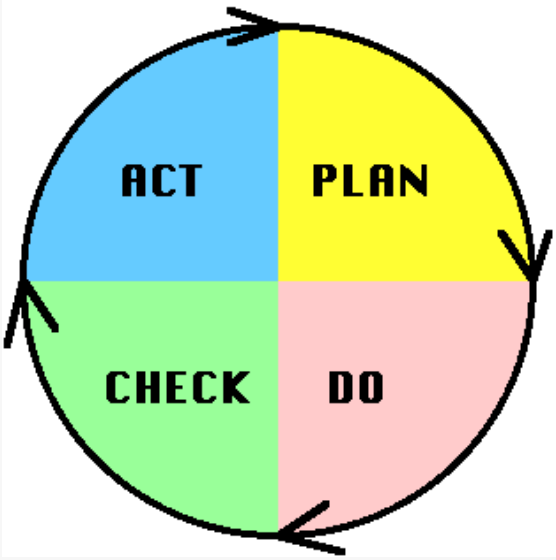
- Efetividade: verifica se os resultados esperados foram obtidos.
- Valor para o negócio: verifica os ganhos / perdas para o negócio.

PDCA

A defesa cibernética envolve um ciclo constante de aprendizado e evolução. A gestão diária dos indicadores, aliada a uma cultura de melhoria constante, reduzirá a chance de sua organização ser exposta em um ataque.

O Ciclo de Deming é uma ferramenta poderosa e alternativa para a gestão e melhoria dos serviços. É proposto um ciclo de acompanhamento contínuo para que os times possam identificar e alterar partes de um processo que necessitem de melhorias. O Ciclo de Deming também é conhecido como PDCA (Erro! Fonte de referência não encontrada.). A Erro! Fonte de referência não encontrada. apresenta um resumo de cada etapa.

Figura 1 – Ciclo de Deming



Fonte: BALANCEDSCORECARD

Tabela 1 - PDCA

Etapa	Descrição
Plan	Planejar as alterações que serão realizadas no serviço visando a melhoria da qualidade.
Do	Implantar as alterações e medir os resultados.
Check	Levantar os resultados e reportá-los para os tomadores de decisão.
Act	Deliberar sobre as alterações necessárias para melhorar o processo.

NOT – Network Operations Center

O NOC (*Network Operations Center*) é uma estrutura com foco no gerenciamento centralizado das redes de dados públicas e privadas de uma organização (LAN, MAN e WAN). O seu principal objetivo é garantir a disponibilidade das comunicações da organização.

O NOC monitora, analisa e controla a disponibilidade e o desempenho de todos os elementos presentes na rede incluindo roteadores, switches e computadores. As principais entregas do NOC estão relacionadas à gestão e ao controle de:

- Tempo de latência.
- Consumo de recursos, incluindo largura de banda, cpu e memória.
- Desempenho dos diversos elementos que fazem parte da rede.
- Desvios e picos de uso.
- Capacidade do ambiente.

SOC – Security Operations Center

O SOC (*Security Operations Center*) mantém o ambiente operacional, garantindo sua atualização e disponibilidade. Os serviços oferecidos normalmente contemplam:

- Detectar incidentes e monitorar o seu status.
- Realizar o diagnóstico inicial, isolando e mitigando o incidente se possível.
- Manter o ambiente operacional:
  - Aplicação de patches.
  - Aplicação de ações corretivas.
  - Aprovação de regras de firewall.
  - Atualização de antivírus.
  - Atualização de whitelist.
  - Aplicação de procedimentos.
  - Administração remota de equipamentos.
  - Atualização de alertas.
  - Envolver e interagir com o próximo nível de resolução (CSIRT, por exemplo).

A lista de serviços oferecidos pode variar em função do escopo requerido pelo negócio e pelas qualificações do time. O SOC pode ser classificado em função da gama de serviços oferecidos e da sua capacidade de atender ataques mais sofisticados.

Primeira geração: contempla basicamente a execução de procedimentos de baixa complexidade. A capacidade da equipe é limitada e a atuação é reativa.

Segunda geração: além de realizar as atividades de primeira geração, é feita a gestão e a correlação entre os eventos e as informações de segurança. Dessa forma, é possível detectar e registrar ataques identificados através da correlação, por exemplo, força bruta.

Terceira geração: realiza as atividades de primeira e segunda geração e agrega atividades de gerenciamento de vulnerabilidades, incluindo a sua detecção, acompanhamento e resolução. Nessa geração, também são executados procedimentos complexos para a solução de incidentes.

Quarta geração: a capacidade de correlação de informações é expandida com a adoção de big data. Diversas ferramentas são empregadas para a detecção, isolamento e solução de uma falha. A capacidade analítica e técnica da equipe são elevadas.

Quinta geração: uso de algoritmos supervisionados (Machine Learning) e não supervisionados (deep learning) para identificação e resposta aos ataques.

CSIRT

O CSIRT (*Computer Security Incident Response Team*) tem sua atuação direcionada para o tratamento de incidentes. É o grupo responsável por prevenir, atuar e gerenciar quaisquer incidentes de segurança. Ele também tem por função fazer o relacionamento com as diversas empresas que o suportam e com a mídia, quando necessário.

Um CSIRT pode oferecer diferentes tipos de serviço para os seus clientes. Tipicamente, eles contemplam atividades ligadas à análise, ao atendimento, ao suporte e/ou à coordenação de incidentes de segurança.

Esses podem ser agrupados em três categorias (exemplos na Erro! Fonte de referência não encontrada.):

Reativos: são os principais serviços do CSIRT. São disparados a partir de um evento ou solicitação.

Proativos: permitem antecipar ou prevenir ataques ou falhas de segurança. Possibilita a redução de incidentes no futuro.

Gerenciamento da qualidade da segurança: são serviços não ligados diretamente ao tratamento de incidentes, que aumentam a segurança de toda a organização. Aumentam também a qualidade dos serviços existentes providos por outras áreas. Usam o conhecimento e a experiência da equipe do CSIRT para a análise de riscos, vulnerabilidades e redução de incidentes futuros.

Tabela 2 – Exemplos de Serviços

<table>
<tr><th>Reativos</th><th>Proativos</th><th>Gerenciamento da qualidade da segurança</th></tr>
<tr><td>Tratamento de alarmes.</td><td>Auditorias e verificações.</td><td>Análise de riscos.</td></tr>
<tr><td>Tratamento de incidentes.</td><td>Gestão das ferramentas de segurança.</td><td>BCM / DRP.</td></tr>
<tr><td rowspan="3">Tratamento de vulnerabilidades.</td><td>Desenvolvimento de ferramentas de segurança.</td><td>Consultoria de segurança.</td></tr>
<tr><td rowspan="2">IDS.</td><td>Treinamentos.</td></tr>
<tr><td>Avaliação de produtos.</td></tr>
</table>

> Capítulo 2

Capítulo 2. Governança Corporativa

A segurança da informação é essencial na longevidade das empresas. A adoção conjunta aos demais frameworks de governança de TI torna a empresa menos suscetível à concorrência e a tropeços. Este capítulo apresenta o conceito de governança e de alguns frameworks complementares.

Na medida em que as empresas cresceram, tornou-se necessária a dispersão da propriedade, gerando profundas mudanças estruturais. Os proprietários saíram do dia a dia e o delegaram para executivos contratados, que atuavam sob sua supervisão. Os executivos tinham que equilibrar os interesses pessoais com os interesses dos acionistas. Consequentemente, os objetivos dos gestores das empresas deixaram de se limitar à maximização dos lucros dos proprietários.

O distanciamento dos acionistas levou às inadequações no relacionamento e o conflito de interesses. Esses conflitos geraram a necessidade de adoção de medidas de governança corporativa, que na prática representaram a reaproximação dos donos às empresas.

Os conflitos de agência são uma consequência natural do distanciamento da propriedade e da gestão. Existem dois axiomas fundamentais para o entendimento desse assunto:

O axioma de Klein descreve que é impossível realizar um contrato completo. O grande número de ocorrências imprevisíveis possíveis e a multiplicidade de reações a cada nova ocorrência tornam inviável a criação de um contrato que trata todas as alternativas possíveis.

O axioma de Jensen-Meckling descreve que é impossível ter um agente perfeito que seja neutro entre maximizar os próprios objetivos ou os de terceiros. Nesse caso, numa situação em que estão em jogo

interesses pessoais e interesses do acionista, ele priorizará os resultados próprios.

O Instituto Brasileiro de Governança Corporativa define governança corporativa como “o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre acionistas/cotistas, conselho e administração, diretoria, auditoria independente e conselho fiscal.

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 o acesso ao capital e contribuindo para a sua longevidade”. O grande desafio da governança é equilibrar os interesses dos diversos envolvidos garantindo a continuidade do negócio e a geração de valor para os acionistas.

O foco preliminar da governança é a análise dos objetivos das companhias, considerando o relacionamento entre as demandas e os constituintes da organização (*stakeholders*).

Os *stakeholders* são pessoas, grupos ou instituições com interesses legítimos, que afetam ou podem ser afetados pelas ações praticadas pela empresa. Os *stakeholders* são classificados em quatro grupos:

- *Shareholders*: proprietários, investidores.
- Internos: responsáveis pela geração e monitoramento dos resultados (empregados, executivos, auditores, conselhos).
- Externos: integrados à cadeia de negócio (credores, fornecedores, integrantes da cadeia de suprimentos, clientes e consumidores).

- Entorno: restrito (comunidade onde a empresa está inserida) e abrangente (governos, ONGs, sociedade como um todo).

Valores da Governança

A governança tem um conjunto de valores fundamentais que integram práticas, conceitos e processos:

- *Fairness* (senso de justiça): equidade no tratamento dos acionistas, respeitando o direito dos minoritários e majoritários, além do senso de justiça com os demais *stakeholders*.

- *Disclosure* (transparência): transparência das informações que impactam nos negócios, incluindo resultados, riscos e oportunidades.

- *Accountability* (responsabilidade): prestação responsável de contas, respeitando as melhores práticas de contabilidade e auditoria e garantindo confiabilidade na gestão.

- *Compliance* (conformidade): conformidade no cumprimento das normas reguladoras, contratos e políticas.

Os valores da governança estarão sempre presentes em quaisquer conceitos de governança corporativa, conforme apresentado na Figura 2. Deve-se ressaltar que esses são universais e se aplicam a quaisquer localidades, culturas ou tipologias das empresas.

Figura 2 – Valores e Conceitos da Governança Corporativa

Governança Corporativa Aplicada em TI

A Governança Corporativa aplicada em TI apresenta os seguintes objetivos:

- Obter vantagem da capacidade (skill) de TI para gerar novos modelos de negócio e mudar práticas de negócio.
- Balancear os custos crescentes de TI e a expansão do valor da informação, a fim de obter apropriado retorno do investimento.
- Gerenciar os riscos de fazer negócios em um mundo digital e a consequente dependência de entidades além do controle direto da empresa (serviço de DNS, e-mail externo).
- Gerenciar o impacto de TI na continuidade do negócio.
- Manter a habilidade de TI.
- Construir e manter o conhecimento essencial para sustentar e ampliar o negócio.
- Prevenir falhas de TI, aumentando o valor e a reputação da empresa.

A governança corporativa e a governança de TI têm os mesmos objetivos, em prática: equilibrar os interesses dos stakeholders e aumentar o valor para o shareholder.

A TI precisa estar alinhada à estratégia e aos objetivos das corporações, garantindo a implantação dos projetos e a sustentação do negócio.

Nas próximas seções, descreveremos alguns dos principais frameworks aplicáveis ao dia a de uma operação.

COBIT

O COBIT (*Control Objectives for Information and related Technology*) foi lançado em 1996 pelo ISACA (http://www.isaca.org), com o objetivo de ser uma ferramenta para a auditoria do ambiente de TI. O COBIT 2019, sua versão mais atualizada, é definido como um modelo de controle que atende os requisitos de governança de TI e garante a integridade da informação e dos sistemas de informação. Ele se integra com os principais frameworks do mercado, permitindo o controle afim da empresa.

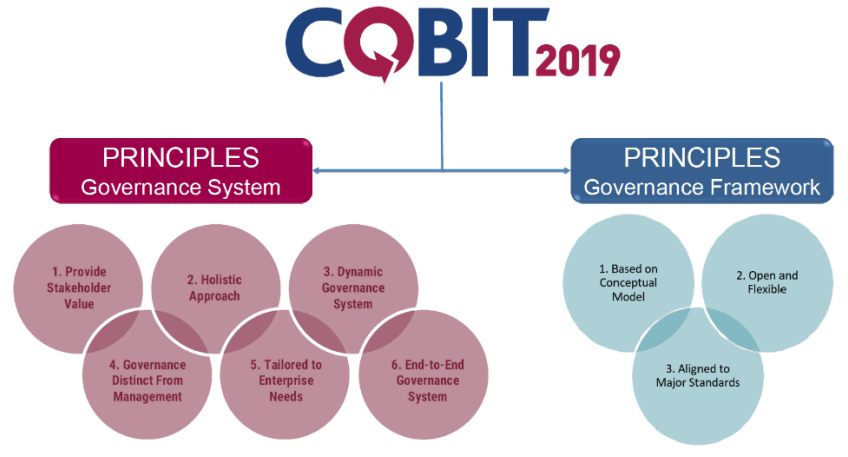
O COBIT 2019 é aberto e flexível, podendo ser adaptado às necessidades de cada empresa. Ele é facilmente integrável a outros frameworks de mercado, servindo como uma importante ferramenta de auditoria. O seu modelo conceitual foi planejado de forma integrada com as interfaces, processos e conceitos claramente definidos, facilitando a automação e integração de processos.

A governança do COBIT 2019 ampara-se nos seguintes princípios (Erro! Fonte de referência não encontrada.):

- Agregar valor ao shareholder.
- Promover uma visão holística, abordando todos os aspectos necessários para a boa governança da empresa.
- Prover um sistema de governança dinâmico e adaptável às mudanças do negócio.
- Separar o gerenciamento da governança, garantindo que as atividades e decisões sejam executadas de acordo com a estratégia organizacional traçada.
- Adaptar-se à realidade da empresa.

- Visão fim a fim contemplando os diversos aspectos necessários para a governança de TI de uma organização.

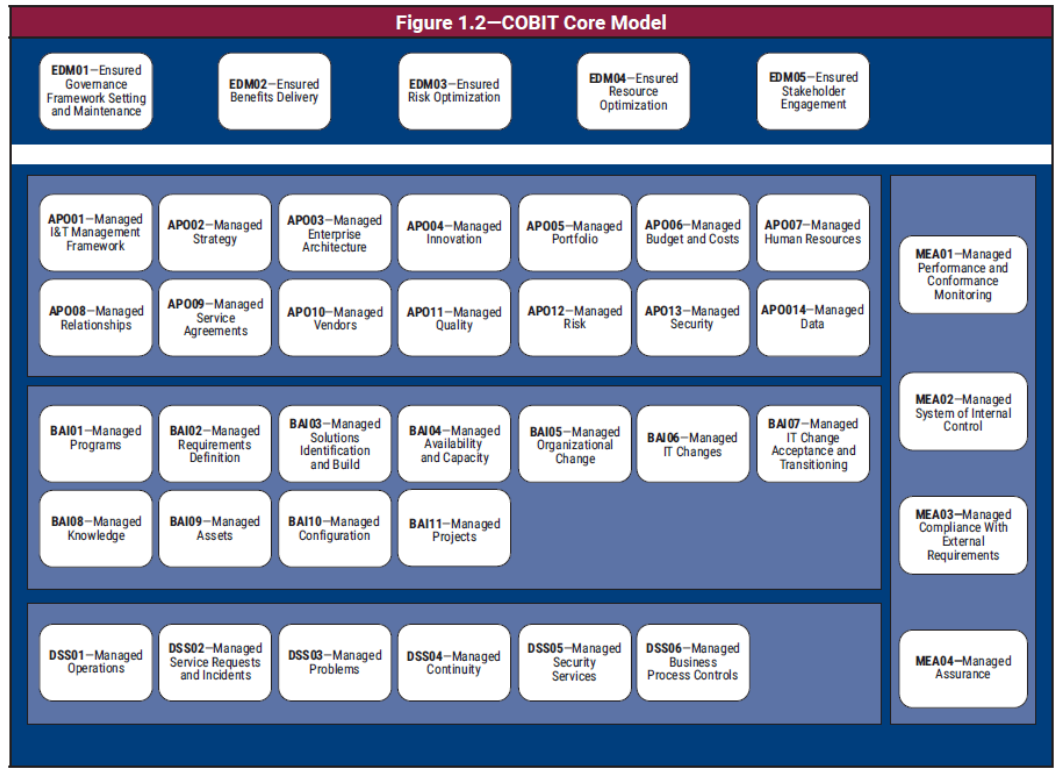
Figura 3 – Princípios do COBIT 2019



Fonte: ISACA, 2018.

A Erro! Fonte de referência não encontrada. apresenta os domínios de conhecimento do COBIT e os seus processos:

Figura 4 – Estrutura do COBIT 2019.



O(a) aluno(a) interessado(a) poderá se cadastrar gratuitamente no site do ISACA (https://www.isaca.org/) e acessar diversas publicações do COBIT e de materiais relacionados à segurança da informação.

ITIL

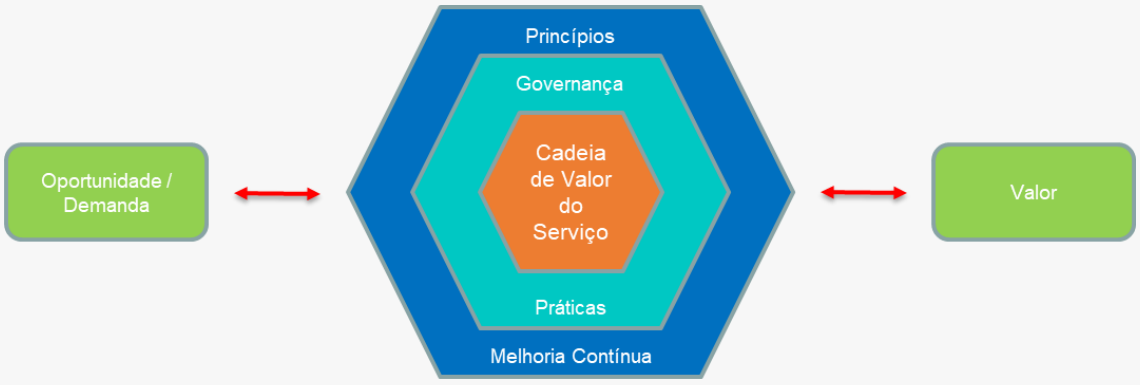
O ITIL (*IT Information Library,* 2019) é um conjunto das boas práticas para o Gerenciamento do Ciclo de Vida dos Serviços de TI. Ele está na versão 4 (atualizada em 2019) e é amplamente utilizado pelos diversos setores da economia e do governo. O *framework* foi desenvolvido pelo OGC e é mantido pelo ITSMf (http://www.itsmfi.org/). O ITIL (2019) pode ser utilizado livremente sem o pagamento de direitos autorais. Ele também não tem uma característica prescritiva, podendo ser adaptado para a realidade da empresa.

O ITIL (2019) define um serviço como sendo um meio de criação de valor conjunto ao valor, facilitando os resultados que os clientes querem alcançar e sem assumir os custos e riscos. Para isso acontecer, alguns princípios devem ser respeitados:

- Foco na criação conjunta de valor. Essencial entender o cliente e suas reais necessidades.
- Entenda o cenário atual. Práticas, culturas e ferramentas já existentes podem te auxiliar.
- Faça as entregas em sprints. Mantenha a evolução constante e adapte-se juntamente à empresa.
- Trabalhe em conjunto com o seu cliente.
- Não existe TI sem o negócio.
- Seja simples e não simplista. Busque um MVP (*Minimum Viable Product*).
- Otimize e automatize o que for necessário.

O ITIL define um Sistema de Valor de Serviço (Erro! Fonte de referência não encontrada.) englobando práticas que visam garantir a criação do valor percebido pelo cliente:

Figura 5 – ITIL - Sistema de Valor de Serviço



Fonte: AXELOS, 2019.

- As oportunidades, demandas e valor são o gatilho para tudo que ocorre na organização.

- A governança controla e direciona a organização de TI.
- As práticas são um conjunto de recursos organizacionais projetados para executar um trabalho ou alcançar um objetivo.
- A melhoria contínua promove a evolução e os níveis sustentáveis de serviço.

PMBOK

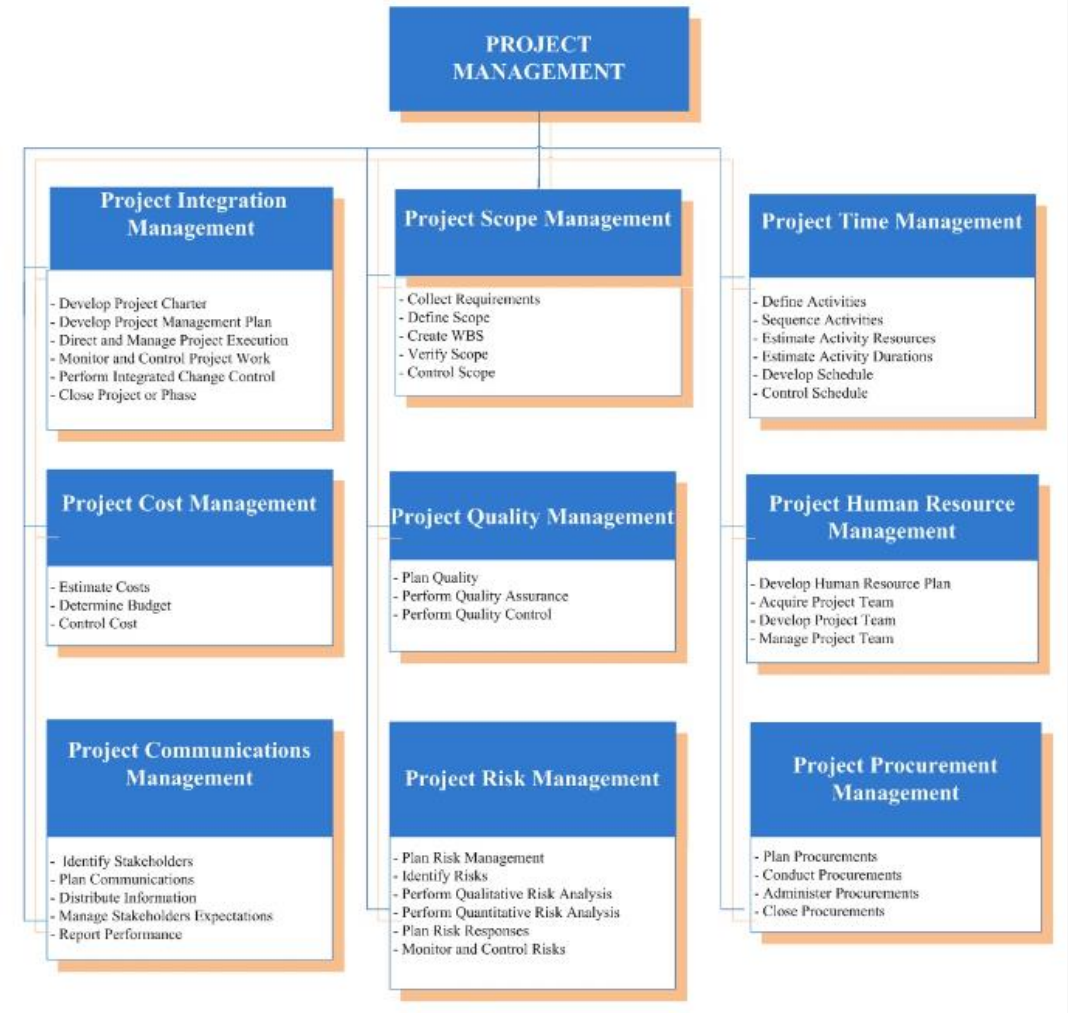
O PMBOK (*Project management body of knowledge*) é focado na excelência em gerenciamento de projetos. Segundo esse *framework*, um projeto é um esforço temporário para criar um serviço ou produto ou resultado exclusivo. Ele necessita de objetivos claros, parâmetros de medição, datas de início e de término que atendam aos requisitos das partes interessadas (*stakeholders*).

O PMBOK tem como principais objetivos:

- Padronização das atividades e fluxos do gerenciamento do projeto.
- Assertividade na comunicação.
- Controle e gestão das atividades importantes.
- Eficiência do uso de recursos.
- Controle do projeto e da sua evolução.
- Mitigação de riscos.
- Aumentar chances de sucesso do projeto.

O PMBOK (http://www.pmi.org) define um conjunto de áreas de conhecimento e processos que contemplam as diversas dimensões envolvidas no gerenciamento efetivo de um projeto (Erro! Fonte de referência não encontrada.).

Figura 6 – PMBOK: áreas de conhecimento e processos



Fonte: pmi.org

> Capítulo 3

Capítulo 3. ISO27000

A família ISO 27000 contempla mais de 40 normas que versam sobre a governança da segurança da informação em TI. Como resultado da implantação, são esperados que todos os tipos de organização (por exemplo, empresas comerciais, agências governamentais e organizações sem fins lucrativos) obtenham:

- Proteção a seus ativos de informação.
- Padronização dos termos.
- Introdução aos sistemas de gestão de segurança da informação (ISMS).
- Breve descrição do processo *Plan do check act* (PDCA).
- Compreensão de termos e definições que estão em uso em toda a família de normas.

ISO27001: Modelo focado em estabelecer, implantar, operar, monitorar, rever, manter e melhorar um sistema de Gestão da Segurança da Informação.

ISO27002: Código de prática para segurança da informação. Ele define os objetivos e os controles da segurança da informação.

ISO27005: Provê orientação em identificação, levantamento, avaliação, e tratamento dos riscos de segurança da informação.

Sistema de Gestão da Segurança da Informação (SGSI)

A ISO 27001 determina a implantação de um SGSI, visando garantir a CIA (*Confidentiality, Integrity, Availability*). A norma recomenda:

- A forma como as políticas devem ser escritas no SGSI e revisadas para conformidade.
- A estrutura da organização de segurança com os papéis e responsabilidades.
- Como as pessoas são informadas sobre a segurança da informação durante o seu ciclo na organização.
- Os processos para a proteção dos dados, incluindo o controle de hardware, software e bancos de dados.
- O controle do acesso aos dados.
- Como será feita a criptografia dos dados confidenciais.
- Os processos para a segurança física dos equipamentos e edifícios.
- Os processos para coleta e armazenamento dos dados.
- Os sistemas de comunicação e os mecanismos para proteção dos dados.
- Os processos para aquisição, desenvolvimento e manutenção de sistemas de acordo com os padrões de segurança.
- As questões envolvidas na contratação de entidades externas e como elas influenciam na segurança do ambiente.
- As práticas de gerenciamento dos incidentes de segurança.
- Aspectos necessários para garantir a continuidade dos negócios em caso de um incidente de segurança.
- Conformidade com as leis e regulamentos relevantes para a organização.

O SGSI define e implanta estratégias, planos, políticas, medidas, controles usados para a definição, implantação, operação, monitoração e evolução da segurança da informação numa organização.

A norma determina a adoção do modelo PDCA (*Plan, Do, Check, Act*) para a implantação do SGSI.

- Plan: definir o SGSI contemplando seu escopo, objetivos e políticas.
- Do: implantar o SGSI considerando ferramentas, políticas, controles e processos, treinamentos e tudo que for necessário para a correta operação e gestão do processo.
- Check: monitorar continuamente e analisar os resultados da implantação considerando auditorias regulares, acompanhamento de indicadores, levantamento de desvios, análises de tendências.
- Act: promover a melhoria contínua executando ações corretivas e preventivas, aplicando as lições aprendidas e comunicando as alterações.

ISO27005

A ISO 27005 é uma norma para avaliação e gestão de riscos de segurança da informação alinhada com a ISO 27001. O gerenciamento de risco tem 6 etapas principais (ISO27005):

- Estabelecimento do contexto: define os critérios para identificação de riscos, papeis e responsabilidades, critérios para identificar como os riscos afetam a confidencialidade, integridade e disponibilidade das informações e critérios para cálculo do impacto e probabilidade.
- A avaliação de risco contempla as etapas:
    - Listar os ativos.

- Identificar as ameaças e vulnerabilidades associadas a cada ativo.
- A partir dos critérios estabelecidos, calcular o impacto e a probabilidade.
- Avaliar os riscos para cada ativo e sua aceitabilidade.
- Priorizar os riscos a serem tratados.

- O tratamento de riscos apresenta quatro alternativas:
  - Eliminar o risco totalmente.
  - Alterar o risco aplicando controles e mitigando o risco.
  - Transferir o risco com terceiros (seguro ou terceirização).
  - Aceitar o risco se estiver dentro dos limites aceitáveis (critérios de aceitação alinhados aos interesses dos acionistas).

Deve-se promover a comunicação entre todas as partes envolvidas no processo de gerenciamento de risco. Dessa forma, será possibilitado o compartilhamento das informações, decisões e o contexto que as cerca. A comunicação deve ser estruturada e implantada de acordo com um plano de comunicação previamente acordado, garantindo sua efetividade e regularidade.

O sucesso da iniciativa dependerá da monitoração constante do ambiente. Os riscos podem ser alterados rapidamente. Nesse sentido, deve-se monitorar a inclusão de novos ativos ao ambiente, mudanças no negócio, novas ameaças internar ou externas e incidentes de segurança.

> Capítulo 4

Capítulo 4. Governança de Dados

O direito à privacidade, ou seja, o direito a ser esquecido é a base da governança e privacidade de dados. As sessões a seguir exploram esse contexto.

Proteção e Privacidade de Dados e Dados Pessoais

A segurança de dados visa a proteção das informações digitais em todo seu ciclo de vida contra corrupção, acesso não autorizado ou roubo. Deve-se considerar todas as dimensões envolvidas, tais como: segurança física dos equipamentos, processos, políticas, gestão de acessos, segurança lógica, controles de hardware, controles administrativos, gestão de acesso e segurança lógica de aplicativos de software.

A LGPD (Lei Geral de Proteção de Dados, 2018) versa no artigo 2º que:

- Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

> I - O respeito à privacidade;
> II - A autodeterminação informativa;
> III - A liberdade de expressão, de informação, de comunicação e de opinião;
> IV - A inviolabilidade da intimidade, da honra e da imagem;
> V - O desenvolvimento econômico e tecnológico e a inovação;
> VI - A livre iniciativa, a livre concorrência e a defesa do consumidor;
> VII - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

O foco da segurança de dados é a gestão do ciclo de vida dos dados, dando visibilidade à organização sobre onde e como os dados da

organização são usados. Visando garantir esses controles, deve-se buscar ferramentas capazes de aplicar as tecnologias abaixo, bem como garantir os requisitos de monitoração e de auditoria.

- Criptografia: adota-se um algoritmo para codificação dos dados de forma que apenas usuários com a chave correta consiga ler as informações.
- Apagar dados: garante que os dados sejam permanentemente eliminados dos dispositivos impedindo a sua recuperação. Nesse caso, sobrescreve-se a informação tornando inviável qualquer tentativa de leitura.
- Mascaramento de dados: os dados reais são alterados de forma a impedir a identificação pessoal permitindo o teste dos aplicativos e o treinamento das equipes com dados reais.
- Resiliência de dados: os dados são distribuídos em diferentes locais permitindo a sua recuperação, mesmo em caso de uma falha massiva numa localidade ou dispositivo.

Existem diversas estratégias para garantir a segurança dos dados. Deve-se, entretanto, considerar não apenas os aspectos tecnológicos. Todo o time de tecnologia, os demais departamentos da empresa e os clientes devem ser constantemente treinados e os processos devem ser revisados. Deve-se também considerar alguns pontos críticos:

- Garantir o treinamento constante do time e de todos os envolvidos.
- Realizar backups e testes de restore das informações e aplicações, zelando pela sua segurança.
- Segurança física dos diversos elementos que compõem o seu ambiente on-premise, nuvem e dos usuários.

- Garantir que os acessos sejam concedidos apenas às pessoas de direito e que sejam limitados às suas necessidades.
- Garantir a política e a implantação dos patches de segurança dos sistemas operacional e dos aplicativos.
- Sempre monitorar e evoluir a monitoração do ambiente.

Princípios da Governança de Dados

A governança de dados controla o ciclo de vida dos dados na organização, incluindo papéis e responsabilidades; quem, quando e como pode acessar e/ou manipular processos e ferramentas.

O Data Governance Institute (DGI) determina oito princípios:

- Integridade de todos os envolvidos no processo, discutindo abertamente motivadores, restrições, opções e impactos das decisões.
- Transparência nos processos e decisões.
- Processos, controles e decisões auditáveis.
- Definir claramente o dono (accountable) das decisões que envolvem dados comuns a diversos elementos da organização.
- Definição do dono (accountable) pelas atividades de administração dos dados.
- Definição do dono (accountable) por verificar e garantir as necessidades de negócio e tecnológicas, padrões e requisitos de conformidade.
- Garantir o suporte e padronização de dados corporativos.

- Garantir a consistência dos dados na medida em que forem manipulados e operados.
- As empresas possuem estruturas próprias para a governança dos dados. Deve-se ao menos garantir a existência desses três elementos:
- Comitê gestor: um comitê executivo que definirá o direcionamento estratégico para a governança dos dados na organização garantindo a aplicação e execução das políticas definidas.
- Dono dos dados: Garante a precisão e consistência dos dados, aprovando alterações na estrutura, auditando as informações e eficiência e efetividade dos processos.
- Administrador de dados: Opera o dia a dia identificando e corrigindo falhas, executando as tarefas de rotina e gerenciando o ambiente.

O artigo 5º da LGPD (2018) contempla o seguinte ciclo de vida dos dados:

Figura 7 – Ciclo de Vida dos Dados

- Coleta: dados pessoais devem obedecer ao princípio da finalidade e necessidade.
- Processamento: será realizado apenas de acordo com o artigo 7º.
- Análise: a análise deve ser feita de acordo com a finalidade da coleta.
- Compartilhamento: os dados serão compartilhados apenas se previamente autorizado pelo titular.
- Armazenamento: Os dados serão mantidos por prazos definidos.
- Reutilização: um novo consentimento será necessário sempre que a finalidade for alterada.
- Eliminação: os dados serão eliminados após o término do tratamento.

> Capítulo 5

Capítulo 5. Direito Digital

O direito digital é uma evolução do próprio Direito. Ele considera os mesmos princípios fundamentais vigentes, apenas incluindo novos elementos. Na prática, o mundo digital não é tratado separado do mundo físico.

O direito à privacidade remete aos anos de 1890, quando foi publicado na Harvard Law Review, o ensaio “The right to privacy”, de autoria de Samuel Warren e Louis Brandeis (FIA). No trabalho, cunhou-se a expressão “direito de ser deixado em paz” — *right to be let alone* (WARREN, 1890).

A Declaração Universal dos Direitos Humanos (ONU, 2021) aborda, entre diversos tópicos, que todas as pessoas são protegidas pela lei e que não podem sofrer ataques a sua honra e reputação. A declaração também garante a liberdade de expressão.

No ano de 2011, foi promulgada a Lei de Acesso à Informação (LAI, 2011), Lei Nº 12.527. Ela define que as informações dos órgãos públicos devem ser, por padrão, de livre acesso e o sigilo exceção. O acesso será restrito apenas em casos específicos, por determinação legal ou judicial. A administração pública, nas esferas federais, estaduais e municipais, deverá publicar, sem solicitação prévia, informações de interesse coletivo. A lei é aplicada aos três poderes (Executivo, Judiciário e Legislativo), Ministério Público e Tribunais de Contas. As entidades privadas, quando receberem e empregarem recursos públicos, deverão também seguir ess00a legislação.

A Lei 12.735, também conhecida como Lei Carolina Dieckmann (LCD, 2012), foi publicada em 2012 e criminaliza os seguintes atos:

- Invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
- Produzir, oferecer distribuir, vender ou difundir dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida acima.
- Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.
- Falsificação de documento particular.
- Falsificação de cartão.

O Marco Civil da Internet (MCI), lei Nº 12.965, publicado em 2014 estabelece os fundamentos para o uso da internet no país e as diretrizes para a atuação da união, estados e municípios. A lei garante:

- Respeito à liberdade de expressão nos princípios da constituição.
- Proteção da privacidade e de dados pessoais.
- Direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais.
- Pluralidade e a diversidade.
- Abertura e a colaboração.
- Livre concorrência, iniciativa e a defesa do consumidor.
- Neutralidade de rede.

- Direito de acesso à internet a todos.

LGPD – Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD), Lei Nº 13.709 foi promulgada em 2018. Ela é aplicada a todas as organizações que tratam os dados de cidadãos brasileiros. Ela tem como fundamentos:

- Respeito à privacidade.
- Autodeterminação informativa.
- Liberdade de expressão, de informação, de comunicação e de opinião.
- Inviolabilidade da intimidade, da honra e da imagem.
- Desenvolvimento econômico e tecnológico e a inovação.
- Livre iniciativa, a livre concorrência e a defesa do consumidor.
- Respeito aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A LGPD (2018) estabelece os seguintes princípios para os dados pessoais:

- Finalidade: realização do tratamento apenas no escopo previamente aprovado pelo titular.
- Adequação: compatibilidade do tratamento das informações com a finalidade aprovada.
- Necessidade: limitação da coleta de dados ao mínimo necessário para a realização de suas finalidades.

- Livre acesso: o titular pode, a qualquer momento, consultar na sua integralidade todos os seus dados pessoais.
- Qualidade dos dados: os dados devem ser exatos, claros, relevantes e atualizados dos dados de acordo com a finalidade.
- Transparência: acesso garantido aos titulares das informações armazenadas sobre ele.
- Segurança: garantia de proteção dos dados impedindo acessos e divulgações não autorizadas.
- Prevenção: adoção de medidas proativas focando na prevenção de danos em virtude do tratamento de dados pessoais.
- Não discriminação: garantir a privacidade impedindo o uso das informações para fins discriminatórios ilícitos ou abusivos.
- Responsabilização e prestação de contas: o agente deve garantir e comprovar o cumprimento das normas de proteção dos dados.

A LGPD (2018) determina que toda empresa tenha um encarregado pelo tratamento de dados pessoais. Esse deve:

- Gerir reclamações, esclarecimentos e garantir as medidas indicadas pelo titular.
- Ponto de contato para a autoridade nacional e adotar as providências necessárias.
- Garantir o treinamento e orientação de funcionários e terceiros.
- Garantir a execução das normas e determinações.

A LGPD (2018) determina também um programa de governança de dados contemplando:

- Comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento da legislação.
- A aplicabilidade em todos os dados sob seu controle.
- Compatibilidade com a estrutura, escala e o volume de suas operações, bem como à sensibilidade dos dados tratados.
- Políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade.
- O estabelecimento de relação de confiança com o titular a partir de atuação transparente e que assegure mecanismos de participação do titular.
- Integração à sua estrutura geral de governança, estabelecendo e aplicando mecanismos de supervisão internos e externos.
- Planos de resposta a incidentes e remediação.
- Atualização constante com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.
- Efetividade de seu programa de governança em privacidade quando apropriado, atendendo a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

> Capítulo 6

Capítulo 6. Crimes Virtuais

Os crimes virtuais são atividades criminosas que visam ou usam um dispositivo computacional (computador, rede ou um dispositivo). Esses, assim como os crimes comuns, têm conduta que infringe a legislação, sendo culpáveis.

TATEOKI cita alguns exemplos de crimes virtuais: ameaça, crimes contra a honra, induzimento e instigação ou auxílio a suicídio, furto, falsificação de documentos, estelionato, espionagem industrial, violação de segredo, apologia de crime, racismo, atentado a serviço de utilidade pública, pornografia infantil, corrupção de menores, violação de direitos de autor, inserção de dados falsos em sistema de informações, crimes contra equipamentos de votação, invasão de dispositivo informático.

Principais tipos

As técnicas e tecnologias utilizadas variam constantemente. A lista abaixo extraída do site da ENISA (2020) apresenta os principais tipos de ataques vigentes:

- Malware: software malicioso que visa danificar dados ou atuar no ambiente computacional de terceiros sem autorização.
- Ataques via Web (*Web-based Attacks*): usam fragilidades do ambiente ou código para acessar informações sigilosas ou afetar o funcionamento de um serviço. Existem diversas técnicas disponíveis:
  - Cross-site scripting (XSS): um código malicioso é inserido em um site confiável para obter dados indevidamente.

- Injeção de SQL (SQLI): um código malicioso é enviado num formulário de entrada possibilitando a alteração, remoção ou disponibilização dos dados para o invasor.
- Path traversal: injeção de dados na hierarquia do webserver permitindo o acesso à configuração, credenciais e informações armazenadas localmente.
- Inclusão de arquivo local: execução de um arquivo em outro lugar no sistema.
- Negação de serviço distribuída (DDoS). Um serviço é inundado com requisições provenientes de diversos lugares limitando o acesso dos usuários legítimos.

- Phishing: roubo de dados usando alguma mensagem chamativa para atrair a vítima.
- SPAM: envio de mensagens publicitárias não solicitadas.
- Roubo de identidade: uso das informações de outra pessoa para cometer crimes.
- Data Breach: um invasor externo consegue acesso a dados sensíveis, protegidos ou confidenciais.
- Insider Threat: ameaças conduzidas por pessoas da própria organização com acesso privilegiado.
- Botnets: conjunto de equipamentos infectados que poderão de forma orquestrada realizar um ataque.
- Roubo, manipulação, danos e perda de equipamentos.
- Information Leakage: fraqueza da aplicação, em que a mesma revela dados sensíveis.

- Ransomware: tipo de ataque que sequestra seu computador codificando os dados e exigindo pagamento para a sua liberação.
- Espionagem virtual: ato de obter de forma não autorizada informações sensíveis de quaisquer tipos de entidades (governos, empresas, entre outros) visando vantagens comerciais, militares etc.
- Cryptojacking: uso de dispositivos alheios para a mineração não autorizada de cripto moedas para o atacante.

Como se proteger

O CERT.BR apresenta uma cartilha de segurança bastante detalhada e com linguagem acessível. O leitor poderá encontrar o link nas referências.

O blog TMB (2018) apresenta uma lista de 10 mandamentos de segurança:

- Qualquer pessoa ou organização pode ser alvo de cibercriminosos. Esteja ciente e consciente o tempo todo.
- As senhas devem ser individuais, fortes e exclusivas.
- Mantenha todo o software e hardware atualizados.
- Relate toda e qualquer atividade suspeita.
- Proteja todos os dispositivos, incluindo smartphones.
- Identifique pontos fracos de segurança e corrija-os.
- Tenha cuidado ao clicar em links ou arquivos.
- Bloqueie o seu dispositivo quando estiver longe dele.

- Revise suas medidas de segurança cibernética regularmente.
- Faça vários backups, com pelo menos um mantido fora do local (e claro, o proteja).

WHARTON (2016) também oferece uma alternativa de mandamentos que trazem alguns pontos complementares:

- Desenvolva e mantenha uma forte higiene cibernética: treinamento do seu pessoal, políticas de senha, atualização de software, processos atualizados etc.
- Conheça e proteja os seus fornecedores.
- Identifique e proteja os ativos mais críticos.
- Pratique o seu plano de resposta a incidentes de segurança.
- Crie e desenvolva um plano de comunicação.
- Audite externamente e atualize seu plano de resposta de incidentes regularmente.
- Crie um time robusto de monitoração de ameaças de segurança.
- Avalie a possibilidade de fazer um seguro contra-ataques cibernéticos.
- Engaje-se na comunidade de segurança.
- Garanta o conhecimento e aplicação das leis e mantenha o relacionamento com os órgãos competentes.

> Capítulo 7

Capítulo 7. Entidades de Apoio

Existem diversos órgãos que podem oferecer suporte no combate ao crime cibernético. O primeiro passo para qualquer denúncia é coletar todas as evidências possíveis das ações incluindo logs, prints etc. Na sequência, deve-se abrir o Boletim de Ocorrências em uma delegacia especializada e solicitar a remoção do conteúdo indevido.

Seguem alguns sites de referência:

- Lista de delegacias especializadas em crimes virtuais: https://new.safernet.org.br/content/delegacias-cibercrimes.
- Safernet – entidade de defesa dos direitos humanos na internet: https://new.safernet.org.br/.
- Cert Brasil – Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil: https://cert.br.
- Agência Nacional de Proteção de Dados: https://www.gov.br/anpd/pt-br

> Capítulo 8

Capítulo 8. Tratamento de Incidentes

O *National Institute of Standards and Technolo*gy (NIST) propõe o seguinte ciclo de vida para o tratamento de um incidente de segurança (Erro! Fonte de referência não encontrada.).

Figura 8 – Ciclo de vida de um incidente

Fonte: NIST80061

A fase de preparação contempla a definição e implantação de todos os aspectos necessários para a detecção e a análise de um incidente, incluindo: contratação e treinamento das pessoas, estabelecimento de processos, implantação de ferramentas para análise e detecção, documentações, criação de checklists, telefones para escalação dos executivos, ferramentas para logs, configuração do ambiente etc.

A fase de detecção e análise contempla:

- Identificação da ameaça idealmente por uma ferramenta de monitoração.
- Registro do incidente com todas as informações necessárias para o seu tratamento.

- Priorização do tratamento em função do impacto e urgência e encaminhamento para o grupo responsável pela solução.

- Notificação do incidente para os grupos indicados, incluindo: executivos, grupos solucionadores, órgãos de segurança pública etc.

A contenção do incidente é essencial para minimizar possíveis impactos na organização. Deve-se, nesse caso, ter um conjunto de medidas previamente acordadas e treinadas para cada um dos tipos de ameaça. Deve-se também considerar a possibilidade de, apesar do incidente ter sido contido, ainda gerar perdas futuras de dados, em função, por exemplo, de um código malicioso inserido no dispositivo. O controle e monitoração constantes são essenciais até a total eliminação da causa raiz.

Durante a contenção, deve-se também levantar todas as informações necessárias para a identificação do ataque e ofensor, de forma que posteriormente, sejam usadas no processo legal. O leitor interessado pode encontrar maiores detalhes no documento *"Guide to Integrating Forensic Techniques into Incident Response"*. O link de acesso está nas referências. Dentro do possível, e sem atrasar a erradicação da falha, deve-se levantar as informações para a identificação do atacante. Reforça-se a necessidade de primeiro eliminar o impacto e depois, se possível, identificar o mesmo.

Uma vez que o incidente tenha sido contido, deve-se erradicá-lo e recuperar o ambiente. Nesse caso deve-se, de maneira ordenada e planejada, realizar as ações de curto, médio e longo prazo necessárias para a recuperação completa do ambiente. É importante direcionar as ações em função do seu ganho esperado e esforço requerido.

A avaliação pós incidente é essencial para o sucesso da organização. Algumas perguntas deverão ser respondidas:

- O que realmente aconteceu (visão interna e externa)?
- Quando aconteceu? Qual é a linha do tempo fim a fim?
- Qual etapa não funcionou bem? Por quê?
- O que funcionou bem? Por quê?
- Poderíamos ter evitado esse incidente? Onde falhamos?
- Como resolver cada uma das falhas acima? Quanto tempo? Quanto custa?
- Eliminamos definitivamente e em todo o parque a ameaça? Qual o plano de ação?

A formalização e o acompanhamento do plano de ação até o seu final são tão importantes quanto o tratamento do próprio incidente.

Referências

ALVES, Gervânia. Ciclo de Vida dos Dados e LGPD. *XPOSITUM*, c2021. Disponível em: <https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd>. Acesso em: 10 ago. 2022.

ANTHONY. 10 Cyber Security Commandments. *TMB*, 14 ago. 2018. Disponível em: <https://blog.tmb.co.uk/cyber-security-commandments>. Acesso em: 10 ago. 2022.

AVERSON, Paul. The Deming Cycle. *Balanced Scorecard Institute*, c1998-2021. Disponível em: <https://balancedscorecard.org/bsc-basics/articles-videos/the-deming-cycle/>. Acesso em: 10 ago. 2022.

AXELOS. *ITIL® Foundation ITIL 4 Edition*. TSO. 2019.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Casa Civil, 2011.

BRASIL. *Lei nº 12.735, de 30 de novembro de 2012*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Casa Civil, 2012.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Secretaria-Geral da República, 2014.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Secretaria-Geral da Presidência da República, 2018.

CARTILHA de Segurança para Internet. *CERT.BR*, 2021. Disponível em: <https://cartilha.cert.br/>. Acesso em: 10 ago. 2022.

CICHONSKI, Paul et al. *Computer Security Incident Handling Guide*. EUA: NIST800-61, ago. 2021. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. Acesso em: 10 ago. 2022.

DEMING, W. Edwards. *O método Deming de Administração*. 5a. Ed., São Paulo: Marques Saraiva, 1989.

DIREITO Digital (Guia Completo): tudo que você precisa saber. *FIA*, 4 out. 2018. Disponível em: <https://fia.com.br/blog/direito-digital/#:~:text=%C3%89%20chamada%20de%20Marco%20Civil,mundial%20de%20computadores%20no%20pa%C3%ADs>. Acesso em: 10 ago. 2022.

ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. *Enisa*, 20 out. 2020. Disponível em: <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>. Acesso em: 23 fev. 2022.

ISACA. *COBIT® 2019 Framework: Governance and Management Objectives.* ISACA. 2018.

ISO27705. *Step-by-step explanation of ISO 27001/ISO 27005 risk management.* Disponível em: <https://advisera.com/27001academy/free-downloads/>. Acesso em: 10 ago. 2022.

KENT, Karen et al. *Guide to Integrating Forensic Techniques into Incident Response*. EUA: NIST800-86, ago. 2006. Disponível em:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>. Acesso em: 10 ago. 2022.

LAWRENCE, David N. et al. 'Tem Commandments' of Cyber Security Can Enhance Safety. *K@W*, 24 fev. 2016. Disponível em: <https://knowledge.wharton.upenn.edu/article/how-the-ten-commandments-of-cyber-security-can-enhance-safety/>. Acesso em: 10 ago. 2022.

MALDONADO, V. Nóbrega. LGPD - *Lei Geral de Proteção de Dados Pessoais Manual de Implementação.* Thomson Reuters, 2019.

MUNIZ, J.; MCINTYRE, G.; ALFARDAN, M. *Security Operations Center – Building, Operating and Maintaining Your SOC.* Cisco Press. 2016.

OLAVSRUD, Thor. Data governance: A best practices framework for managing data assets. *CIO*, 18 mar. 2021. Disponível em: <https://www.cio.com/article/3521011/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.html>. Acesso em: 10 ago. 2022.

ONU. Organização das Nações Unidas. *Declaração Universal dos Direitos Humanos da ONU*. Disponível em: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Acesso em: 10 ago. 2022.

ROSSETI, José Paschoal. *Governança Corporativa: fundamentos, desenvolvimentos e tendências*. 5. ed. Atlas, 2011.

TATEOKI, Victor Augusto. Classificação dos Crimes Digitais. *Jusbrasil*, 2015. Disponível em: <https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais>. Acesso em: 10 ago. 2022.

TZU, S. *A Arte da Guerra*. São Paulo: Record, 2006.

VERIZON. *Data Breach Investigations Report* 2020. Disponível em: <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>. Acesso em: 10 ago. 2022.