A segurança da informação protege a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios, minimizando os danos aos negócios e maximizando o retorno dos investimentos e oportunidades. **(Norma ABNT ISO/IEC 27002)**

ABNT NBR ISO/IEC 27001:2013 (ISO 27001, 2013): - Tríade CID

Confidencialidade: é a propriedade de que a informação não esteja disponível ou seja revelada a indivíduos, entidades ou processos não autorizados.

Integridade:é a propriedade de salvaguarda da exatidão e completeza de ativos.

Disponibilidade: diz respeito à eficácia do sistema e do funcionamento da rede para que seja possível utilizar a informação quando necessário.

Pilares da S.I

Autenticidade: busca garantir que determinada pessoa ou sistema é, de fato, quem ela diz ser;

Não-Repúdio (Irretratabilidade): busca-se garantir que o usuário não tenha condições de negar ou contrariar o fato de que foi ele quem gerou determinado conteúdo ou informação;

Legalidade: O aspecto de legislação e normatização.

Elementos do risco - definições

A gestão de riscos e a definição do risco são imprescindíveis para a segurança da informação.

Quais os elementos que devem ser mapeados, analisados e avaliados? O ativo possui riscos e são os elementos a serem protegidos.

O **agente de ameaça é aquele que explora uma vulnerabilidade.**
Pode ter a intenção e utiliza um método que visa a explorar intencionalmente uma vulnerabilidade, como é o caso de um cracker que utiliza técnicas de ataques para atacar o ativo.

O **agente de ameaça** pode também ser uma situação ou método que permite acidentalmente disparar uma vulnerabilidade, como é o caso do administrador de sistemas que configura de uma forma incorreta (e vulnerável) o servidor de banco de dados.

A **vulnerabilidade** corresponde a uma falha ou fraqueza em procedimentos de segurança, design, implementação ou controles internos de sistemas, que pode ser disparada acidentalmente ou explorada intencionalmente, resultando em brecha de segurança ou violação da política de segurança do sistema, que existe em ativos.

Os **controles de segurança ou os mecanismos de defesa**, devem ser aplicados em vulnerabilidades para evitar que sejam explorados pelos agentes de ameaça.

Já a **ameaça** é o potencial de um agente da ameaça explorar uma vulnerabilidade específica, acidental ou intencionalmente. Uma negação de serviço e o vazamento de informações são exemplos de ameaças.

Quando isso ocorre, a ameaça se torna um **incidente de segurança**, o que resulta em impactos para a organização.

O cálculo da probabilidade disso tudo acontecer representa o risco, segundo cálculo **R=P*I**, no qual **R**=Risco, **P**=Probabilidade e **I**=Impacto.

Ativos envolvidos no projeto, não se esquecendo que eles podem ser as pessoas, os equipamentos e artefatos físicos, os processos e os sistemas e tecnologias. Não é necessário citar todos, mas uma boa representatividade é importante;

Considere crackers e concorrentes como agentes de ameaça. Cite uma ameaça de cada tipo que afeta a confidencialidade, integridade e disponibilidade.

Controles de segurança

Sua Missão Você irá detalhar os seguintes elementos:

Pontos de ataques, representados por sistemas compostos por diferentes aspectos, que possuem vulnerabilidades: hardware, software, protocolos, aplicações;

Pontos de ataques indicando os ativos humanos e físicos envolvidos;

Agentes de ameaça, ameaças e técnicas de ataques;

Controles de segurança para a autenticação dos usuários;

Controles de segurança de rede

CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo **NIC.br, do Comitê Gestor da Internet no Brasil**.
É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. (CERT, 2020).

SCAN - Notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

WORM - Notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

DoS (Denial of Service) - Notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede

Invasão - Um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

Web - Um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

Fraudes - Qualquer ato enganoso, de má-fé com o intuito de lesar outrem, incidentes em que ocorre uma tentativa de obter vantagem.

Outros - Qualquer notificação que não se enquadra nas categorias anteriores

obs: como tudo passa pela rede e a aplicação está na sétima camada de protocolos TCP/IP, o portal de fornecedores está sujeito a vulnerabilidades de rede e de hardware

Lei Geral de Proteção de Dados Pessoais (LGPD)

Com a **Lei Geral de Proteção de Dados Pessoais (LGPD),** os dados pessoais devem ser protegidos para a garantia da privacidade.

Ataques podem ser realizados para **vazar dados pessoais e comprometer a privacidade**, e ataques podem ocorrer com dados em processamento (DIU), dados em transmissão (DIM) ou dados armazenados (DAR).

Ataques a **banco de dados visam os dados armazenados**, enquanto ataques à rede visam os **dados em transmissão**. Já os **dados em processamento** podem sofrer ataques mais sofisticados.

Agentes de Ameaça, Ameaças e Técnicas de Ataques

Os agentes de ameaça são elementos importantes para oentendimento dos riscos e da segurança.

Os **agentes de ameaça mais comuns são as pessoas**, que possuem facetas diferentes, de acordo com o ambiente em avaliação.
Por exemplo, os crackers, um funcionário mal-intencionados, fraudadores.

Há ainda os **agentes de ameaça naturais**, que podem comprometer a disponibilidade da informação em caso de uma inundação de datacenter.

Um agente de ameaça bastante crítico, que pode ser considerado também uma ameaça, é o **malware, ou ocódigo malicioso**.
Malwares são programas desenvolvidos com o objetivo de gerar alguma ação danosa ou maliciosa em um computador

Ataque - DOS Denial of service: é a negação de serviço ou o processo que torna um sistema ou aplicação indisponível. Ex.:um ataque pode ser feito por meio do bombardeamento de solicitações que consomem todos os recursos disponíveis do sistema ou da transmissão de dados de entrada defeituosos que podem acabar com o processo de uma aplicação. Exploração de recursos de maneira agressiva, impossibilitando usuários de utilizá-los. **SYN Flooding**: causa o overflow da pilha de memória e **Smurf**: envio de pacotes específicos.

Controles de Segurança e Proteção - DMZ

A **proteção à rede** considera que, no fluxo da informação, todo acesso passa pela rede, sendo este, portanto, um bom local para controles de segurança.

Uma boa estratégia de segurança deve levar em consideração a rede, com uma arquitetura de redes segura, considerando segmentação, uso de **zonas desmilitarizadas (DeMilitarized Zone, DMZ), controle de acesso de rede e detecção de ataques (OLIVEIRA, 2017).**

A **técnica de DMZ** é uma rede específica que fica entre uma rede pública como a internet e a rede interna. Com esta segmentação, a rede interna conta com uma camada adicional de proteção, pois os acessos são permitidos para os serviços disponibilizados na DMZ, mas não para a rede interna.

Controles de Segurança e Proteção - Firewall

O controle de segurança mais famoso é o **firewall,** que é o responsável pelo controle de acesso de rede.

Na realidade, o firewall começou funcionando na camada de rede, e atualmente ele atua também na camada de aplicação, realizando a proteção contra ataques que vão além de ataques de rede, com o **Web Application Firewall (WAF).**

Enquanto um firewall faz a filtragem do tráfego de rede baseado nos cabeçalhos dos pacotes, o **WAF** faz o filtro e monitora o tráfego entre os usuários e a aplicação Web, na camada de aplicação HTTP

IDS – Sistemas de Detecção de Intrusão/ IPS - Sistemas de Prevenção de Intrusão

IDS - Permitem a detecção de ataques em andamento.

Monitoramento e análise das atividades dos usuários e dos sistemas. Análise baseada em assinaturas de ataques conhecidos

Análise estatística do padrão de atividade Funcionam de uma forma mais ativa que um IDS

IPS -Após a detecção de atividades suspeitas, tomam ações diretas, como o término daquela conexão.

Atua de uma forma in-line, de modo similar ao firewall.

Os sistemas de detecção e prevenção de intrusão atuais incorporam técnicas de inteligência artificial para diminuir a quantidade de falsos positivos (alarmes falsos) e falsos negativos (ataques não detectados).

Antimalware

Antimalware **buscam códigos maliciosos**, e basicamente funcionam com a verificação de assinaturas ou códigos que identificam um malware já identificado anteriormente e que possuem vacina específica.

Se por um lado os códigos maliciosos podem alterar seu próprio código ou gerar polimorfismo para não serem detectados pelo antimalware, do outro lado o controle de segurança adota cada vez mais a inteligência artificial para detectar comportamentos anômalos que podem representar perigo para as empresas.

Criptografia

Da origem para ocultar o significado de uma mensagem até o uso em aplicações como WhatsApp e acesso a websites, passando pelo uso em guerras e por agentes secretos, a criptografia evoluiu de uma arte para uma ciência, e atualmente faz parte de nossas vidas, incluindo os objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, além de dinheiro digital (NAKAMURA, 2016).

A criptografia deriva de duas palavras gregas: kryptos, que significa oculto, e graphien, que significa escrever.

Arte de escrever ou resolver códigos.

Ocultar o significado da informação.

Antes: o objetivo inicial era a comunicação secreta

Atualmente: autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, etc.

Criptografia básica: simétrica ou de chave privada. Chave secreta é a mesma para a cifragem e decifragem, e deve ser compartilhada; Cifragem com algoritmos matemáticos.

Sigilo: proteção dos dados contra divulgação não autorizada. Autenticação: garantia que a entidade se comunicando é aquela que ela afirma ser. Integridade: garantia que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada. Não-repúdio: garantia que não se pode negar a autoria de uma mensagem. Anonimato: garantia de não rastreabilidade de origem de uma mensagem.

Criptografia - Objetivos

Sigilo: proteção dos dados contra divulgação não autorizada.

Autenticação: garantia que a entidade se comunicando é aquela que ela afirma ser.

Integridade: garantia que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada.

Não-repúdio: garantia que não se pode negar a autoria de uma mensagem.

Anonimato: garantia de não rastreabilidade de origem de uma mensagem.

Segurança dos sistemas criptográficos

Geração de chaves: geração aleatória de chaves;

Mecanismo de troca de chaves: chaves precisam ser distribuídas e trocadas para o estabelecimento das comunicações seguras;

Taxa de troca das chaves: quanto maior a frequência de troca automática das chaves, maior será a segurança;

Tamanho da chave: são diferentes para a criptografia de chave privada ou simétrica e para a criptografia de chaves públicas ou assimétricas.

Técnicas de criptografia

A criptografia é baseada em um conjunto de técnicas que incluem a cifragem, funções de hash e assinaturas digitais.

A escolha da técnica depende de critérios: Nível de segurança requerido, métodos de operação dos algoritmos, desempenho, facilidade de implementação.

Criptografia de chave privada

Enviar uma mensagem cifrada

- algoritmo criptográfico
- chave secreta privada para cifrar a mensagem original.

Na mensagem cifrada recebida

- Mesma chave secreta para decifrar a mensagem.

Criptografia de chave pública

- Utiliza um par de chaves para a troca de mensagens
- Chave pública: para cifrar a mensagem.
- Chave privada: decifrar a mensagem (chave exclusiva do receptor).

Esteganografia

Uso de técnicas para ocultar a existência de uma mensagem dentro de outra.

Diferença entre a criptografia e esteganografia

- Uma oculta o significado da mensagem, enquanto a outra oculta a existência da mensagem.

Exemplos: Inserção de mensagens nos bits menos significativos de áudios ou imagens; uso de caracteres Unicode que se parecem com conjunto de caracteres ASCII

Assinatura digital

A mensagem é “cifrada” com a chave privada - validar a origem de uma mensagem

Utiliza a chave pública correspondente para realizar a validação da assinatura.

Cybersecurity, CIS Controls e família NBR ISO/IEC 27.000

Segurança de Informação

Há um **conjunto de frameworks e normas** que guiam as ações de segurança da informação, como as da família NBR ISO/IEC 27000 (ABNT, 2020), que você deve conhecer para organizar e otimizar sua estratégia de segurança da informação.

Além da família NBR ISO/IEC 27.000 há o Cybersecurity Framework do **National Institute of Standards and Technology (NIST)** (NIST, 2018) e o CIS **Controls, do Center for Internet Security (CIS)** (CIS, 2020).

Aspectos normativos e de cultura da segurança da informação, que tratam, de uma **forma integrada**, de processos, pessoas e tecnologias

obs: a segurança é um conjunto de pessoas, processos e tecnologias, sendo as pessoas a parte mais fraca desses 3.

A segurança da informação é direcionada também por **aspectos legais, regulatórios e contratuais**, como os do setor médico, de telecomunicações ou financeiro.

No Brasil a Lei N. 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD) (LGPD, 2020), a Lei N. 12.965, o Marco Civil da Internet (INTERNET, 2014) e a Lei N. 12.737, a Lei Carolina Dieckmann (DIECKMANN, 2012), também reforçam a necessidade de segurança da informação.

Definições:

Obs: Dentro da família 27000, **27001 é a única que possui certificação** da segurança da informação, se a empresa está enquadrada dentro das normas.

Você sabe que pode certificar o SGSI de sua empresa de acordo com a norma ABNT NBR ISO/IEC 27001? A **ABNT NBR ISO/IEC 27002 foca nos objetivos de controles de segurança.**

O **Cybersecurity Framework** possui uma abordagem integrada de diferentes aspectos de segurança importantes.

O **CIS Controls** estabelece uma forma mais prática de trabalho.

A privacidade, que exige a proteção de dados pessoais, o que é regido pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709.

Cybersecurity Framework, do NIST

O Cybersecurity Framework do National Institute of Standards and Technology (NIST) (NIST, 2018) **organiza diferentes elementos da segurança da informação**, focando no uso de direcionadores de negócios para guiar atividades de segurança cibernética, considerando os riscos de segurança da informação.

Este framework trabalha com os elementos importantes para as atividades destes três níveis, incluindo os **objetivos, as priorizações, orçamentos, métricas e comunicação**.

5 funções (identificar, proteger, detectar, responder e recuperar) que provê uma visão estratégica do ciclo de vida dos riscos de segurança da informação.

As funções possuem **23 categorias** abrangendo resultados cibernéticos, físicos, pessoais e comerciais.

Há ainda as **subcategorias, que são 108 divididas nas 23 categorias**, que são orientações para criar ou melhorar um programa de segurança cibernética, com referências a outros padrões de segurança da informação.

CIS Controls, do Center for Internet Security (CIS)

O **CIS Controls** é um conjunto priorizado de **ações** que, de uma forma integrada, **estabelecem a defesa em camadas** para mitigar os ataques mais comuns contra sistemas e redes.

Com **objetivo de melhorar o estado de segurança**, o CIS Controls muda a discussão de “o que minha empresa faz?” para “o que devemos todos fazer?” para **melhorar a segurança e fortalecer uma cultura de segurança da informação**. (CIS, 2020).

Ex.: Classificação como o tamanha das empresas **IG1** são empresas familiares com 10 funcionários. **IG2** uma organização regional e uma grande corporação com milhares de funcionários pode ser classificado como **IG3** (CIS, 2020).

Principais normas e padrões na família 27000

As principais normas e os padrões que envolvem a segurança da informação, são:

Segurança da informação: ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.

Riscos: ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011.

Continuidade de negócios: ABNT NBR ISO/IEC 27031:2015 e ABNT NBR ISO 22301:2013.

Governança de TI: COBIT.

Serviços de TI: ITIL.

Família ISO 27.000 – ISO 27.001

Certificação em segurança da informação pode ser concedida para uma organização que segue a norma ABNT NBR ISO/IEC 27001 (ISO 27001, 2013), que trata dos requisitos de um **Sistema de Gestão de Segurança da Informação (SGSI)**. O auditor líder realiza a auditoria de certificação (BSI, 2020).

Os sistemas de gestão não são tecnológicos, ou necessariamente um sistema automatizado. O sistema é no seu sentido mais amplo, **com o SGSI incluindo estratégias**, planos, políticas, medidas, controles e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a **segurança da informação.**

Família ISO 27.000 – ISO 27.002

A ABNT **NBR ISO/IEC 27002 (ISO 27002, 2013)** é uma norma importante para os profissionais de segurança da informação, ao definir o código de prática para **controles de segurança da informação.** De uma forma geral, a ABNT NBR ISO/IEC 27001 se relaciona com a ABNT NBR ISO/IEC 27002 da seguinte forma:

Escopo da aplicação da ABNT NBR ISO/IEC 27001 é definido;

Análise de riscos é realizado;

Aplicabilidade dos controles de segurança é formalizado;

Controles de segurança são implementados, com base na ABNT NBR ISO/IEC 27002.

Sistema de Gestão de Segurança da Informação (SGSI)

O SGSI é um elemento chave para o fortalecimento da **cultura de segurança da informação das organizações.**

A norma ABNT NBR ISO/IEC 27001 estabelece os requisitos para o estabelecimento de um sistema de gestão de segurança da informação (ISO 27001, 2013).

O **sistema de gestão da segurança da informação** preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

É importante que um SGSI seja parte e esteja integrado com os processos da organização e com a estrutura de administração global e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles (ISO 27001, 2013).

Você deve especificar e implementar o SGSI de acordo com as características específicas da sua organização, que possui necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização.

Como estes fatores evoluem com o tempo, é preciso estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

Esta é uma das características principais dos sistemas de gestão, o processo de melhoria contínua, ou **PDCA (Plan, Do, Check, Act)**

Sistema de Gestão de Segurança da Informação (SGSI)
+ PDCA (Plan, Do, Check, Act)

Plan - (estabelecer) - Estabelecimento da SGSI
Do - (implementar) - Implementação e operação do SGSI
Check - (Manter) - Monitoramento e análise crítica do SGSI
Act - (Melhorar continuamente) - Manutenção e melhoria do SGSI

Partes interessadas - (Do) - Expectativas e requisitos da segurança da informação
Partes interessadas - (Act) - Segurança da informação gerenciada.

Os Requisitos da SGSI são 7

1- Contexto da organização (Qual contexto da organização?)
2- Liderança (Quem são os líderes?)
3- Planejamento (Qual o planejamento que eu tenho?)
4- Apoio (Qual apoio eu tenho?)
5- Operação (Quais operações eu faço?)
6- Avaliação de desempenho (Como está meu desempenho?)
7- Melhoria (Como eu posso melhorar?)

Lei Geral de Proteção de Dados Pessoais (LGPD)

A LGPD (LGPD, 2020) é uma lei que entrou em vigor no Brasil em setembro de 2020, visando proteger os direitos fundamentais de privacidade dos cidadãos brasileiros.,

A lei estabelece **medidas para que haja transparência na coleta e tratamento de dados pessoais** pelas organizações, que deve então prover a proteção adequada destes dados para **garantir a privacidade** dos seus usuários.

Pode acarretar em multa de até 2% do faturamento (até 50 milhões) caso haja falta de transparência com o usuário ou vazamento de dados

De acordo com a LGPD, os dados pessoais podem ser coletados mediante finalidade e base legal.

O titular dos dados pessoais possui direitos, **e a empresa que realiza o tratamento dos dados pessoais** passa a ser o responsável pelos dados pessoais coletados.

E essa responsabilidade envolve, principalmente, a proteção, já que qualquer uso irregular, incluindo o seu vazamento, afeta a privacidade do titular.

As empresas devem, assim, implementar controles de segurança da informação para evitar incidentes de segurança que podem levar ao vazamento de dados pessoais.

Pontos Importantes

A **Lei N. 12.965, o Marco Civil da Internet (INTERNET, 2014)** é a lei que regula o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

A **Lei N. 12.737, também conhecida como Lei Carolina Dieckmann (DIECKMANN, 2012)**, altera o código penal brasileiro, tornando crime a invasão de aparelhos eletrônicos para obtenção de dados particulares, a interrupção de serviço telemático ou de informática de utilidade pública. Há exemplos de crime, penalidade e agravante.

Política de segurança da informação

As políticas de segurança da informação constituem um dos principais controles de segurança da informação.

Com a definição de elementos como regras, orientações, diretrizes, responsabilidades e sanções, as políticas de segurança da informação guiam as ações de todos da organização, incluindo os terceiros, prestadores de serviços, parceiros e fornecedores.

As políticas de segurança da informação devem tratar de todos os aspectos cotidianos da organização, incluindo os relacionados às pessoas, aos processos e às tecnologias.

Cultura de segurança e privacidade

Cultura de segurança - Definições

Toda empresa possui a sua **própria cultura** de segurança e privacidade (COACHMAN, 2010).

O objetivo é que esta cultura seja fortalecida constantemente, principalmente porque cada vez mais a segurança da informação influência na resiliência das empresas.

O grande desafio é que, como toda cultura, a de segurança e privacidade se torna mais forte com ações da empresa que **engajam todas as pessoas**, dos funcionários aos fornecedores. Formada pelo conjunto de hábitos, crenças e conhecimentos em segurança e privacidade as ações devem buscar reforçar estes elementos em todos da empresa.

Fortalecimento da cultura de segurança e privacidade

Treinamento

Conscientização

Tendo a participação ativa da alta administração

A política de segurança e privacidade deve:

1- Refletir as características da empresa

2- Ser plausível e aplicável

3- ser organizada em uma série de documentos

4- ser abrangente, principalmente com agentes externos

5- ser organizada de acordo com o seu público-alvo

6- estar acessível

7- estar sempre atualizada

8- ser comunicada regularmente

Termo ou contrato de confidencialidade

O termo ou contrato de confidencialidade geralmente é utilizado quando há troca de informações, como em prestação de serviços, discussões em que há a necessidade de detalhes da empresa, ou em consultorias.

Garante que há o acesso a informações importantes para a realização da atividade, porém todo o conteúdo deve ser preservado e ser restrito somente à execução das atividades, não podendo ser utilizado posteriormente, e nem divulgado para terceiros.

Assim, este documento é essencial para as relações entre empresas, quando possui acesso a informações sensíveis, e você deve exigir o mesmo quando disponibiliza informações críticas de sua empresa para terceiros.

Segurança da informação na aquisição e desenvolvimento de sistemas

Há diversas alternativas e elas refletem diretamente em como a segurança e privacidade deve ser tratada por sua empresa, principalmente quanto às responsabilidades (BROOK, 2020).

Temos de definir: **Plataforma, Sistema e Aplicação,** se vai ser On-premise, na nuvem ou Saas, onde em cada um terá suas definições próprias

On-premise:

1- Desenvolvimento próprio
2- Contratação de desenvolvimento
3- Software Pronto

Nuvem:

1- Desenvolvimento próprio
2- Contratação de desenvolvimento
3- Software Pronto

Saas:

1- Software pronto

Análises de segurança em diferentes níveis

Análise estática ou Static Analysis Security Testing (SAST); no software em execução, que deve ser analisado em análise dinâmica ou Dynamic Analysis Security Testing (DAST) (KOUSSA, 2018); ou no ambiente de software, em que todos os componentes, incluindo as redes, devem ser analisadas com testes de penetração (penetration testing, **pentest**).

O SAST deve ser **aplicado no código-fonte**, e é importante para **remover as vulnerabilidades do código** antes do software entrar em produção.

O DAST também deve ser realizado antes do software entrar em produção, **e o teste e com o software funcionando**, testando-se as interfaces existentes.

Há ainda um teste de segurança conhecido como **IAST** (Interactive Application Security Testing), que realiza os testes de segurança de uma forma interativa, combinando os testes estáticos e dinâmicos (SAST e DAST).

Armazenamento de dados

Dados

Os dados e a informação estão em fluxo constante e existem em diferentes estados.

Há a transmissão, o processamento, o armazenamento. Estão em meio físico, em meio digital e na cabeça das pessoas.

E os dados e as informações precisam de segurança em todo este fluxo que envolve seus diferentes estados e meios em que existem, naquele momento.

Os dados e a informação estão em fluxo constante e existem em diferentes estados. Há a **transmissão, o processamento, o armazenamento**.

Estão em meio **físico, em meio digital e na cabeça das pessoas**.

E os dados e as informações precisam de segurança em todo este fluxo que envolve seus diferentes estados e meios em que existem, naquele momento.

Estado dos dados em meios digitais: DIU, DAR, DIM

Os dados em meios digitais existem em três estados .

Dados transmitidos, seja em **redes sem fio ou em qualquer tipo de conexão**, **incluindo a internet, são conhecidos com Data-In-Motion (DIM).**

Estes dados podem ser comprometidos durante a transmissão, o que pode comprometer a confidencialidade, integridade ou disponibilidade

Os **dados em processamento são conhecidos como Data-In-Use (DIU)**, que realizam as transformações dos dados necessários para as operações e possibilitam as interações necessárias entre o usuário e o serviço.

Há um espaço limitado de oportunidade para que ataques cibernéticos aconteçam com o DIU, já que as aplicações realizam as operações necessárias, e os dados continuam o seu fluxo, normalmente para o armazenamento.

Os **dados armazenados, conhecidos como Data-At-Rest (DAR),** possuem uma grande exposição aos agentes de ameaça, e recebem grande parte da atenção de segurança.

Porém, é preciso entender que, para que um atacante chegue aos dados armazenados, é preciso passar os ativos que estão custodiando os dados.

Mascaramento, anonimização e pseudonimização

Além da criptografia, há outros controles de segurança que devem ser conhecidos e considerados para serem utilizados para a proteção de dados.

Um dos controles que protegem os dados, limitando a exposição, é o mascaramento de dados.

Com esta técnica, os dados não são expostos em toda a sua totalidade, com apenas trechos que sejam suficientes para as operações.

No contexto do Payment Card Industry Data Security Standard (PCI DSS), o mascaramento é um método **para ocultar um segmento de dados** ao ser exibido ou impresso (PCI, 2014).

Já o **truncamento** é um método que remove permanentemente um segmento dos dados no armazenamento (PCI, 2014).

Caso haja o **armazenamento**, há o truncamento ao invés do mascaramento, que é utilizado apenas na sua exibição ou impressão.

Como no caso do **truncamento** utilizado no armazenamento a remoção é permanente, as substituições podem ser feitas de uma forma mais geral, sem indicar o número de algarismos substituídos.

Anonimização e pseudonimização

Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), **a anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento**, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo .

Já a **pseudonimização é tratada pela lei como sendo o tratamento por meio do qual um dado perde a possibilidade de associação**, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (LGPD, 2020).

Segurança de dados na nuvem

Já no contexto de provedores de nuvem, é preciso atentar para os dados tratados pelo provedor de nuvem, considerando ainda o término do contrato.

De uma forma geral, o uso de um provedor de nuvem envolve o provisionamento, a migração e o desprovisionamento.

Os dados não podem ser acessados indevidamente em nenhum momento pelo provedor de nuvem.

A segurança de dados na nuvem tem um caminho a seguir que é de 14 passos:

1 - Proteção de dados em trânsito
2 - Proteção e resiliência de ativo
3 - Separação entre usuários
4 - Governança
5 - Segurança de cadeia de fornecedor
6 - Desenvolvimento seguro
7 - Segurança pessoal
8 - Segurança operacional
9 - Gerenciamento seguro do usuário
10 - Identidade e autenticação
11 - Proteção das interfaces externas
12 - Administração segura de serviços
13 - Informação de auditoria para usuários
14 - Uso seguro do serviço

Segurança e Auditoria de Sistemas
Segurança na internet, dispositivos móveis e testes de intrusão

Segurança na internet

A segurança e privacidade na internet passa pelo entendimento de diferentes elementos que envolvem o que deve ser protegido e os componentes ou ativos de um ambiente que podem ser explorados em ataques.

Formas e estados do dado e informação/ CID

Trilha de acervo conhecida (Confidencialidade, Integridade e Disponibilidade)

As informações podem estar em diversas formas:

O **dado/informação**, pode estar no estado **físico, digital ou na cabeça das pessoa**s, tais dados ou informações podem **estar em transmissão, em processamento ou armazenadas.**

Transações WEB

As transações Web, que partem dos **usuários,** que utilizam seus dispositivos a partir de algum local em que há uma conexão internet, passam por variados componentes até chegar à loja virtual, ao serviço do governo ou o banco.

Neste caminho, os **agentes de ameaça** estão à espreita em busca de oportunidades para **roubar os dados** pessoais, **dados das transações Web e as identidades digitais**.

Além da exploração de vulnerabilidades, estes agentes de ameaça buscam os **golpes na internet** para o mesmo fim, de ter acesso a informações valiosas .

Segurança na internet

O **agente de ameaça** buscando oportunidades em três ambientes: **no ambiente do usuário, no ambiente de internet que inclui o provedor de internet, e no ambiente dos provedores de serviços, sistemas e plataformas.**

Segurança em transações Web

As **transações Web, realizadas pela internet,** envolvem uma série de questões de segurança que parte do usuário e chegam ao provedor de serviços, como um banco, passando pelo provedor de internet.

Uma **transação Web pode ser uma compra online**, uma **transação bancária**, a realização de algum **serviço governamental** ou até mesmo uma **postagem em uma rede social.**

E as transações podem envolver diferentes tipos de dados ou informações: **dados pessoais, dados financeiros ou dados confidenciais,** que podem sofrer **modificações, vazamentos ou destruições**, afetando, respectivamente, a integridade, **confidencialidade e disponibilidade.**

Transação Web em bancos

Usuário acessa o serviço (Utiliza navegador ou aplicativo em seu dispositivo)

Banco autentica o usuário (Banco valida a identidade digital do usuário com credenciais vindo pela internet)

Usuário realiza uma transação bancária (Usuário realiza a transação utilizando uma senha)

Transação Web em bancos

As ameaças no banco, são o **furto de identidade, a captura da senha, a captura da senha de transação, a modificação da transação e a interrupção do acesso, que podem afetar a autenticação ao serviço, a transação bancária e a autenticação da transação**.

Elas podem ocorrer em qualquer um dos três ambientes **(usuário, internet e provedor de serviços)** e , porém de uma forma diferente, o que leva à necessidade de controles de segurança diferentes, que afetam também as responsabilidades.

No ambiente de internet, em que o agente de ameaça pode capturar ou modificar as transações Web, é importante que elas sejam realizadas com o uso de um canal seguro, que deve ser provido pelo provedor de serviços, como o banco.

As **conexões Web podem ser protegidas** com o uso de protocolos de segurança como o **Hyper Text Transfer Protocol Secure (HTTPS)**.

O HTTPS possibilita o uso do HTTP sobre uma sessão Secured Socket Layer **(SSL)** ou Transport Layer Security (TLS), com a criação de um túnel seguro por onde trafegam as informações.

Além de garantir a **confidencialidade (dados cifrados com chave simétrica de sessão)**, eles podem visar também a integridade dos dados (uso de Message Authentication Code, **MAC**) e a autenticidade das partes (as entidades podem ser autenticadas com o uso de criptografia de chave pública).

Já no ambiente do **provedor de serviços**, como no caso de bancos, o ambiente pode ser atacado em qualquer um dos componentes, incluindo as **aplicações, os servidores de aplicação, os sistemas operacionais, as máquinas virtuais, os bancos de dados.**

O banco é um dos órgãos que mais investem em segurança da informação, alguns dos **golpes mais comuns e extremamente aplicados** são:

Furto de identidade
Fraude da antecipação de recursos
Phishing ou Scam
Pharming
Golpes de comércio eletrônico
Boato ou hoax

Privacidade na Web

A **privacidade na Web** possui visões a serem consideradas. De um lado, há o **rastreamento** do que as pessoas fazem na Web, **como os cookies**.

Do outro, há a **divulgação espontânea de informações pessoais** em redes sociais, que podem resultar em crimes que transcendem o digital e podem afetar diretamente as pessoas com fraudes e crimes diversos.

E, com a Lei Geral de Proteção de Dados Pessoais (LGPD) (LGPD, 2020), todos devem preservar a privacidade e a proteção de dados pessoais.

Segurança e privacidade

Para a **segurança em transações Web,** pensar:

Transação parte do **usuário**, que utiliza dispositivos e possui instalados aplicativos ou aplicações;

Transação **trafega pela internet,** passando pelo **provedor de internet;**

Transação chega à empresa, e os dados são **processados e armazenados;**

Há ameaças **no ambiente do usuário, do provedor de internet e da empresa**;

Se o usuário for comprometido, a empresa também pode ser;

O que pode ser feito para que o usuário não seja comprometido;

O que deve ser feito pela empresa após receber os dados pessoais e transacionais.

O ponto central a ser planejado é que, além dos controles de segurança para proteger a transmissão dos dados dos clientes para a sua empresa, usando HTTPS/TLS/SSL, os clientes são parte central da segurança e privacidade, pois transações fraudulentas podem chegar à em**presa a partir deles.**

Mostre que pode haver o furto de identidade, a captura da senha, a captura da senha de transação, a modificação da transação e a interrupção do acesso. Essas ameaças existem no ambiente do cliente, no ambiente de internet e no próprio ambiente da empresa, que utiliza um provedor de nuvem.

Mostre que, no ambiente do cliente, os golpes na internet potencializam as ameaças, aumentando o nível de risco. E, como é o ambiente com menor controle, o desafio é maior nos clientes.

Apresente os principais golpes na internet que podem comprometer a sua empresa, com destaque para o **phishing e o pharming**.

Defina a partir deste mapeamento um plano de **conscientização para os clientes**, minimizando as probabilidades deles caírem em fraudes na internet, e também de serem vítimas de malwares.

Dentre as dicas, podem ser inclusos pontos como **não clicar em links recebidos por e-mails e SMS**, além de verificar sempre se uma conexão segura está estabelecida com a empresa, verificando os dados do certificado digital.

Usar autenticação **de duplo fator**. Com este controle de segurança, em caso de furto de identidade, ainda é necessário o dispositivo móvel para o acesso aos serviços da empresa, o que torna o acesso indevido mais difícil.

Com relação à **privacidade e proteção de dados pessoais**, oplanejamento deve incluir os avisos de privacidade na coleta das informações dos clientes. Além disso, a proteção destes dados pela empresa é parte da estratégia de segurança e privacidade, com o reforço de que há sanções previstas na LGPD.

Outro ponto importante a ser planejado são os **processos e mecanismos para o atendimento às solicitações dos clientes, que podem consultar e solicitar a remoção dos seus dados pessoais.**

Assim, com o tratamento destes principais aspectos, a sua empresa poderá operar com a necessária segurança e privacidade, **minimizando** os problemas de acessos a partir de clientes falsos, resultando em melhores resultados.

Dispositivos Móveis

São um dos principais **vetores de ataques**, com os criminosos virtuais buscando maximizar seus resultados visando o canal em que há maior número de alvos e possibilidades de sucesso.

Os dispositivos móveis representam um grande desafio para as empresas, já que, além dos **dados corporativos, há os dados pessoais**.

E isso implica no aumento da **complexidade de proteção**, além do intrínseco aumento de riscos.

Ex.: quando um colaborador instala **jogos** em seu dispositivo móvel, mas a partir de fontes não confiáveis.

Riscos no uso de dispositivos móveis no mundo corporativo

O (dispositivo móvel) celular ideal para uso corporativo deve conter

Container: para separação entre contexto de uso pessoal e profissional.
Anti-Malware:
Identificação e remoção de app vulneráveis:
Autenticação de duplo fator, certificado digital e senha:
Uso de criptografia no tráfego:
Conexão apenas de dispositivos confiáveis:

Capacidades de segurança necessárias

Proteção contra o acesso indevido aos dados do dispositivo móvel
Configurações de privacidade para proteger os dados dos usuários
Proteção contra tentativas de phishing
Proteção de dados armazenados no dispositivo móvel
Gerenciamento centralizado para aplicar política e configuração aos dispositivos
Avaliação da segurança dos aplicativos móveis

Engenharia social (acesso as informações pessoais) de dispositivos móveis

O **phishing** conta com a **engenharia social,** que explora a atenção, curiosidade, caridade, medo ou possibilidade de obtenção de vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou site popular.

Envolve a possibilidade de inscrição em serviços de proteção de crédito, ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas

falsas em que entregam suas credenciais, senhas ou informações sensíveis, além da instalação de códigos maliciosos (CERT, 2020).

O usuário recebe um phishing e clica em um link que pode levar a um site onde ele entrega informações pessoais ou as suas credenciais de acesso, ou pode levar à instalação de malware.

Exemplificando

O phishing é explorado também no mundo dos jogos eletrônicos, com os atacantes distribuindo malwares via links em chat de jogos e criando aplicativos falsos que visam ser populares, utilizando inclusive ícones similares para ludibriar as vítimas (SECURITY, 2020)

Um dos malwares, distribuído via mídia social, plataforma de jogos ou chat de jogos, é o **LeifAccess ou o Shopper**, que envia mensagens falsas de alertas para que o usuário **ative serviços de acessibilidade do dispositivo móvel.**

O malware então utiliza as funções de acessibilidade para criar contas, baixar aplicativos e postar mensagens usando a conta da vítima (SECURITY, 2020).

Segurança em dispositivos móveis para empresas

Um dos principais pontos da arquitetura é a definição do modelo a ser adotado, que pode ser a disponibilização de dispositivos móveis somente para o uso corporativo, a permissão para uso pessoal (Corporate-OwnedPersonally-Enabled, **COPE**), ou o Bring Your Own Device (**BYOD**) ou Choose Your Own Device (**CYOD**).

No modelo BYOD ou CYOD, o dono do dispositivo móvel é o próprio usuário, enquanto nos outros a propriedade é a da empresa. O modelo COPE provê flexibilidade de usoao permitir que tanto a empresa quanto o usuário possam instalar aplicativos no dispositivo, que é de propriedade da empresa (NCCoE, 2020).

Algumas recomendações de segurança e privacidade para empresas adotarem no uso de dispositivos móveis são(FRANKLIN et al, 2020):

Conduzir uma análise de riscos em dispositivos móveis e para as informações acessadas por eles;

Adotar tecnologias de segurança móvel como Enterprise Mobility Management (**EMM**), plataformas de defesa contra ameaças móveis ou serviço de veto a aplicações móveis, que utiliza uma variedade de técnicas estáticas, dinâmicas e comportamentais para determinar, com o uso de uma pontuação, se uma aplicação ou dispositivo demonstra qualquer comportamento que representa um **risco de segurança ou de privacidade**.

Prover a segurança em cada dispositivo móvel corporativo antes de permitir o acesso a sistemas e informações corporativas, com **uso de uma solução de gerenciamento de mobilidade** corporativa (EMM/MDM)...

Ciclo de vida, um dos ciclos de vida é dividido em 7 partes:

1- Entender o caso de uso e as capacidades existentes
2- Conduzir uma avaliação de riscos
3- Selecionar a implantação, dispositivo, EMM
4- Definir politica, configuração e provisionamento
5- Testar a verificação
6- Auditar o uso do dispositivo
7- Descarte ou reuso do dispositivo

ANÁLISE DE VULNERABILIDADE E PENTEST

Processos da gestão de vulnerabilidades

A **identificação de vulnerabilidades** é o início dos trabalhos para proteger as empresas, e pode ser feita de diferentes formas. Uma vez descoberta e validadas as vulnerabilidades, elas devem ser tratadas com os **controles de segurança**.

Fluxo da gestão de vulnerabilidades

Descoberta
Priorização de ativos
Avaliação
Relatório
Remediação
Verificação

Todos os ativos possuem vulnerabilidades que temos controle, sejam físicos, tecnológicos ou processuais para tentar eliminar ou minimizar todas as vulnerabilidades.

Testes de segurança

São importantes para a **gestão de segurança da informação** porque identificam as vulnerabilidades, que podem ser assim serem tratadas. E há diferentes formas de realizar testes de segurança e identificar as vulnerabilidades.

O objetivo é a sua empresa disponibilizar serviços seguros, sem as vulnerabilidades. Sem os testes de segurança, a sua empresa pode estar expondo informações sigilosas e a privacidade de clientes, colaboradores e parceiros.

Se a sua empresa **desenvolve software**, deve disponibilizar o sistema de uma forma segura, seguindo práticas que vão eliminando as vulnerabilidades desde o início do desenvolvimento até após a implantação em ambiente de produção.

Se a sua empresa utiliza software de terceiros, deve realizar testes de segurança para garantir que o ambiente da empresa, composta por softwares de diferentes fornecedores e de naturezas diferentes, esteja seguro.

E os testes de segurança são uma das principais atividades de empresas especializadas em segurança e privacidade, com a oferta de serviços de análise de vulnerabilidades e **pentests**, por exemplo.

Há diferentes testes de segurança, como as análises e avaliações de riscos, e as análises de vulnerabilidades, que focam tradicionalmente em aspectos tecnológicos.

Para a Open Web Application Security Project **(OWASP)**, que foca em **aplicações Web,** teste de segurança é o processo de comparar o estado de um sistema ouaplicação de acordo com um conjunto de critérios (OWASP, 2014).

Eles podem ser feitos no final do desenvolvimento, oufazer parte do ciclo de desenvolvimento desde o início, com a implementação de requisitos e testes de segurança automatizados (OWASP, 2019).

Os testes de segurança, que envolvem variáveis como a origem dos testes (interno ou externo), as informações prévias disponíveis para os testes, o uso de ferramentas automatizadas e a qualificação dos profissionais.

Testes Externos: Pentest sendo eles: **Caixa Branca** (White-Box) **Caixa Cinza** (Gray-Box) ou **Caixa Preta** (Black-Box)

Testes Internos: Análises de Vulnerabilidade sendo eles: **Análise estática** (SAST) ou **Análise Dinâmica** (DAST)

Testes de segurança Interno – Análise de Vulnerabilidades

A análise de vulnerabilidades compreende a busca por vulnerabilidades nos ativos de uma forma manual ou com o uso de ferramentas automatizadas, como os scanners. Os tipos de análise de vulnerabilidades são as análises estática e dinâmica (KOUSSA, 2018) (OWASP, 2019).

A análise estática, ou Static Application Security Testing **(SAST)**, envolve a análise dos componentes do sistema sem a sua execução, pela análise manual ou automatizada do código-fonte.

A **análise manual** exige proficiência na linguagem e no framework usado pela aplicação, e possibilita a identificação de **vulnerabilidades na lógica de negócios, violações de padrões e falhas na especificação**, especialmente quando **o código é tecnicamente seguro, mas com falhas na lógica**, que são difíceis de serem detectados por ferramentas automatizadas. Já a análise automatizada é feita com ferramentas que checam o código-fonte por conformidade com um conjunto pré-definido de regras ou melhores práticas da indústria (OWASP, 2019).

A **revisão manual do código** pode ser feita com o uso de métodos mais básicos de busca de palavras-chave no código-fonte, ou com a análise linha-a-linha do código-fonte. Também podem ser utilizados os ambientes de desenvolvimento, ou Integrated Development Environments **(IDEs)** (OWASP, 2019).

A análise dinâmica, ou Dynamic Application Security Testing (**DAST**), envolve a análise do sistema durante a sua execução, em tempo real, de forma manual ou automatizada. Normalmente a análise dinâmica não provê as informações que a análise estática provê, mas detecta elementos sob o ponto de vista do usuário, como os ativos, funções, pontos de entrada e outros.

A análise dinâmica é conduzida na camada da plataforma e nos serviços e Application Programming Interfaces (**APIs**) do backend, que são locais em que as requisições e respostas das aplicações podem ser analisadas.

Os resultados são referentes, principalmente, a problemas de **confidencialidade no trânsito, de autenticação e autorização, além de erros de configuração do servidor (OWASP, 2019).**

O SAST e DAST podem ser adotados pelas próprias equipes de desenvolvimento no contexto do **DevSecOp**, que é um conceito importante que pode ser seguido para o desenvolvimento de software, ao integrar os testes de segurança na esteira de desenvolvimento, envolvendo a integração contínua e a entrega contínua. (CONSTANTIN, 2020)

Pentest

Os **testes de penetração ou pentests**, são também conhecidos como **testes de intrusão e ethical hacking**, e são realizados a partir do ambiente externo.

Os objetivos são determinar “se” e “como” um agente de ameaça pode obter um acesso não autorizado a ativos que afetam um ambiente, e confirmar se os controles requeridos por um padrão, regulamento ou legislação estão implementados.

Envolve ainda identificar meios de explorar vulnerabilidades para driblar os controles de segurança dos componentes do sistema (PCI, 2017).

Há três tipos de pentests, que depende das informações do ambiente obtidas antes dos testes de segurança:

O acesso prévio a informações do ambiente de estado, sendo eles **Caixa Branca** (White-Box) **Caixa Cinza** (Gray-Box) ou **Caixa Preta** (Black-Box), o que diferencia esses 3 testes é a informação que você terá para executar esse teste de invasão.

O **teste de caixa preta (Black-Box)** é também conhecido como **teste com conhecimento zero,** já que é conduzido sem qualquer informação sobre o ambiente que está sendo testado.

O objetivo é que o profissional faça o teste como se fosse um atacante real, explorando o uso de informações públicas e que podem ser obtidas (OWASP, 2019).

O **teste de caixa branca (White-Box)** é também conhecido como teste com conhecimento total, e é **conduzido com todo o conhecimento sobre o ambiente**, que engloba o código-fonte, documentações e diagramas.

Este tipo de teste é mais rápido do que o teste de caixa preta, porque há a transparência e o conhecimento permite a construção de casos de teste mais sofisticados e granulares (OWASP, 2019).

O **teste de caixa cinza (Gray-Box)** é o teste em que **alguma informação é provida para o profissional**, como uma credencial de acesso, enquanto outras informações têm que ser descobertas.

Este teste é bastante comum, devido aos custos, tempo de execução e escopo do teste (OWASP, 2019).

Metodologia OWASP Testing Project

A **OWASP** Testing Project foca em **aplicações Web,** e visa a construção de aplicações mais confiáveis e seguras. A metodologia segue as premissas de que a prática detestar o software deve estar em todo o ciclo de vida de desenvolvimento de software (Software Development Life Cycle, **SDLC)** e que uma das melhores maneiras de prevenir **bugs** de segurança em aplicações em produção é o SDLC incluir a segurança em cada uma de suas fases.

Framework da metodologia da OWASP

1- Antes do desenvolvimento

1- Definição do SDLC
2- Revisão de políticas e padrões
3- Desenvolvimento de métricas

2- Definição e especificações

1- Revisão dos requisitos da segurança
2- Revisão da especificação e arquitetura
3- Criação e revisão dos modelos UML
4- Criação e revisão dos modelos e ameaça

3- Desenvolvimento

1- Execução simulada do código
2- Revisão do código

4- Implantação

1- Pentest da aplicação
2- Testes do gerenciamento de configuração

5- Manutenção e operações

1- Revisão do gerenciamento operacional
2- Checagem periódica
3- Verificação das mudanças

Metodologia PTES

A metodologia Penetration Testing Execution Standard(PTES) é composto por sete seções, que definem as atividades a serem realizadas, desde as interações iniciais até o relatório.

De uma forma geral, as atividades são suportadas por uma documentação técnica detalhada, para cada uma das seções do PTES.

As seções descrevem como iniciar as atividades, obter informações para a análise, a modelagem de ameaças, as análises de vulnerabilidades, a exploração para passar pelos controles de segurança existentes, o pós-exploração para manter o acesso e controle do alvo, e o relatório final.

As sete seções são:

1- Interações iniciais
2- Obtenção das informações
3- Modelagem de ameaças
4- Análises de vulnerabilidades
5- Exploração
6- Pós-exploração
7- Relatório

Relatório

Os testes internos fazem parte do ciclo de vida de desenvolvimento de software, com atividades de segurança sendo realizados nas fases de definição, especificação, desenvolvimento, implantação e manutenção das plataformas **Web e móvel**.

A **análise de vulnerabilidades** no código-fonte, a Static Analysis Security Testing (**SAST)**, será feita por sua equipe. A SASTcomplementará outras atividades de segurança e privacidade importantes durante o desenvolvimento, antes da implantação:

•Treinamento da equipe em segurança e privacidade;

•Revisão de políticas e padrões de segurança e privacidade; Uso de métricas para medir a segurança e privacidade das plataformas Web e móvel;

•Revisão dos requisitos de segurança, incluindo mecanismos como gerenciamento de usuários, autenticação, autorização, confidencialidade de dados, integridade, contabilidade, gerenciamento de sessão, segurança no transporte, segregação em camadas, conformidade com legislação e padrões;

•Revisão da especificação e arquitetura;

•Criação e revisão integrada dos modelos UML;

•Criação e revisão do modelo de ameaças;

•Execução simulada do código; •Teste do gerenciamento de configuração.

Outro teste de segurança a ser realizado antes da implantação, com a plataforma Web e móvel em execução, é a Dynamic Analysis Security Testing (DAST).

Normalmente a análise dinâmica não provê as informações que a análise estática provê, mas detecta elementos sob o ponto de vista do usuário, como os ativos, funções, pontos de entrada e outros.

Após a implantação do sistema, o plano é a contratação de uma empresa especializada em pentest, para complementar os testes feitos pela sua própria equipe.

A empresa contratada fará o teste de caixa preta, com uma visão total do agente de ameaça, enquanto a sua equipe fará o teste de caixa branca, que faz sentido pela sinergia existente com os outros testes de segurança da fase de desenvolvimento, com o acesso ao código-fonte, documentação e diagramas.

Conceitos e Princípios

Auditoria

A auditoria de sistemas é cada vez mais importante para as empresas e tem como papel assegurar que os controles internos sejam eficientes e efetivos.

A segurança da informação e privacidade, que é feita a partir de uma visão de riscos que direciona a definição e implantação de controles de segurança, é uma das áreas em que a auditoria é parte essencial para garantir que a empresa esteja de fato protegida contra as ameaças.

Auditoria - Objetivos

A auditoria tem como objetivo verificar e validar atividades, processos e sistemas das empresas de acordo com o que está estabelecido, incluindo aspectos legais e regulatórios, visando também a eficiência e eficácia.

Ela é feita em diferentes contextos, como o ambiental, contábil, financeiro, fiscal, riscos, segurança, sistemas, social, tributário ou trabalhista. Outro objetivo da auditoria é atestar a conformidade com regulações administrativas, regulatórias e legais.

Segundo a Information Systems Audit and Control Association (ISACA), que foca em sistemas de informação, a auditoria é uma inspeção e verificação formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se os objetivos de eficiência e eficácia estão sendo alcançados (ISACA, 2016).

Ciclo da Auditoria

Validar atividades, processos e sistemas
Avaliar a eficiência e eficácia dos controles
Atestar a conformidade administrativa, regulatória e legal
Assegurar para a alta gestão e diferentes atores a estabilidade organizacional.

Inspeção e verificação formal

Padrão ou conjunto de guias está sendo seguido?
Objetivos de eficiência e eficácia estão sendo atingidos?
Os registros estão corretos?

Auditoria de sistemas

Pode detectar problemas em:

Fraudes em e-mail;
Uso inadequado de hardwares;
Fraudes, erros e acidentes;
Vazamento de informações;
Falta de segurança física (acessos indevidos).

Benefícios da Auditoria de Sistemas

Superação de resistências a tecnologia;
Avaliação, escolha e implantação de softwares e hardwares;
Gerenciamento dos arquivos eletrônicos;
Maior transferência de conhecimento;
Independência das limitações impostas pelos arquivos de auditoria em papel;
Maior produtividade.

Auditoria de Segurança e Controles de Segurança

Para a segurança e privacidade das empresas, é importante que os processos estejam bem definidos e a equipe responsável tenha as competências para as ações necessárias.

A governança garante que as ações do cotidiano sejam tratadas de modo que as ameaças correntes e as emergentes sejam sempre tratadas e alinhadas com a alta gestão (ISACA, 2017).

Os investimentos em controles de segurança são necessários para proteger as empresas contra os ataques cibernéticos, que estão crescendo em sofisticação e abrangência. Somada à necessidade regulatória, a segurança da informação e privacidade faz parte da estratégia e framework das empresas, o que leva à necessidade de revisão gerencial, avaliação de riscos e auditoria dos controles de segurança (ISACA, 2017).

Os investimentos para melhorar a proteção e as respostas aos incidentes são definidos nos programas de segurança e privacidade das empresas

Do ponto de vista da alta gestão, as questões envolvemos valores investidos, se eles estão adequados e se foram direcionados e implementados corretamente, também em comparação com os concorrentes.

Com isso, há dois elementos importantes para as empresas: a avaliação dos riscos atuais e emergentes para a empresa e a auditoria dos controles de segurança atuais e que estão planejados para protegerem os ativos da empresa.

Assim, a gestão de riscos é importante para identificar, analisar e avaliar os riscos, que direcionarão a definição dos controles para o tratamento dos riscos. Com a auditoria, a empresa assegura que os controles protegem a empresa de uma forma adequada.

Auditor

Uma das principais características da auditoria é que ela só pode ser feita por auditores, os quais são profissionais que normalmente têm certificação para exercer esta função.

Outra característica é que a auditoria é independente das funções operacionais, o que permite que sejam providas opiniões objetivas e sem viés sobre a efetividade do ambiente de controle interno (ISACA, 2016).

ITAF

Information Technology Audit Framework (ITAF) da ISACA é um framework de auditoria de TI que define padrões para as auditorias de TI relacionadas aos papéis e responsabilidades, ética, comportamento esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto.

Além disso, o ITAF provê guias e técnicas para planejar, executar e reportar auditoria de TI (ISACA, 2020).

Information Technology Audit Framework (ITAF) da ISACA é um framework de auditoria de TI que define padrões para as auditorias de TI relacionadas aos papéis e responsabilidades, ética, comportamento esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto.

Além disso, o ITAF provê guias e técnicas para planejar, executar e reportar auditoria de TI (ISACA, 2020).

A auditoria requer que o auditor busque evidências, avalie as forças e fraquezas de controles internos com base nas evidências coletadas e prepare um relatório de auditoria que apresenta as fraquezas e recomendações para a remediação de uma forma objetiva para apresentar aos atores envolvidos.

Fases da Auditoria

As fases do processo de auditoria são importantes, com o planejamento, trabalho em campo e relatórios.

O mais importante é, porém, o conhecimento do auditor, que precisa definir as técnicas e as ferramentas para a auditoria, a qual exige conhecimentos amplos e profundos para que seja possível fazer uma análise da eficiência e eficácia dos controles da empresa.

A efetividade da auditoria depende, em grande parte, da qualidade do programa de auditoria.

No caso da auditoria de controles de segurança, há a exigência de um conjunto de habilidades que envolvem aspectos especializados, tais como para os pentests, as análises de configurações de servidores ou firewalls, a revisão de regras de ferramentas de segurança (ISACA, 2017).

Plano de auditoria e programa de auditoria

Plano de auditoria:

1- Stakeholders
2- Objetivo
3- Escopo
4- Entregáveis
5- Orçamentos
6- Alocações de recursos
7- Data da agenda
8- Tipo de relatório e audiência
9- Metodologia

Programa de auditoria

1- Conjunto de procedimentos e instruções para testar os controles, avaliar os resultados, obter evidências e reportar os resultados
2- Áreas a serem auditadas
3- Ferramentas e técnicas utilizadas para testar os controles

Principais fases de um processo de auditoria e os passos

Planejamento

1- Determina o objetivo da auditoria
2- Define o objetivo da auditoria
3- Estabelece o escopo da auditoria
4- Executa o planejamento da pré-auditoria
5- Determina os procedimentos

Trabalho em campo

1- Adquire dados
2- Testar controles
3- Realizar descobertas e validação
4- Documenta resultados

Relatórios

1- Segue requisitos dos relatórios
2- Elabora relatórios
3- Entrega relatórios
4- Acompanha

Principais fases de um processo de auditoria e os passos

Você trabalha para um provedor de nuvem em franca expansão, que tem demandas diretas de seus clientes.

Eles exigem cada vez mais segurança e precisam estar em conformidade legal e regulatória, o que significa que só se tornarão clientes caso o próprio provedor esteja em conformidade com as melhores práticas de segurança e tecnologia da informação.

O planejamento, assim, precisa incluir um elemento que aumente a confiança dos potenciais clientes, os quais precisam de um provedor seguro para operar seus sistemas e dados.

O planejamento segue os itens gerais:

Como é a segurança do provedor de nuvem, em linhas gerais: a segurança segue os processos essenciais de identificação, proteção, detecção, resposta e recuperação São processos importantes para que a confidencialidade, integridade e disponibilidade dos dados e informações dos clientes sejam maximizados.

A segurança é feita com base nos riscos, que é a probabilidade de um agente de ameaça explorar vulnerabilidades de um ativo, fazendo com que uma ameaça se torne um incidente de segurança, o que resulta em impactos para a empresa.

Os controles de segurança são identificados e implantados com base nos riscos avaliados, com este tratamento dos riscos envolvendo ainda os riscos aceitos.

Por que a segurança é importante, focando nos clientes: os clientes demandam a segurança porque precisam proteger seus negócios, e o provedor de nuvem operará seus sistemas e dados. Além disso, há a necessidade de conformidade legal e regulatória, exigida para todo o setor.

Demanda dos clientes para a conformidade: a conformidade é baseada em regulamentos e leis, como a do setor financeiro, que exige proteção dos ativos tecnológicos, e a do setor de saúde, que exige a segurança e privacidade dos dados dos pacientes, por exemplo.

O conjunto de controles deve ser verificado sob a óptica destas necessidades legais e regulatórias e atestado pelo auditor.

Auditoria de segurança, por que fazer: os controles de segurança implantados podem não ser eficientes e eficazes, o que compromete a segurança do provedor de nuvem e de todos os seus clientes. Além disso, riscos não identificados podem não estar sendo tratados. A auditoria é necessária para validar atividades, processos e sistemas; avaliar a eficiência e eficácia dos controles; atestar a conformidade administrativa, regulatória e legal; e assegurar para a alta gestão e diferentes atores a estabilidade organizacional. estabilidade organizacional.

Principais fases da auditoria:

(1) planejamento, que envolve principalmente a definição do escopo e das técnicas e ferramentas a serem utilizadas na auditoria;

(2) trabalho em campo, em que dados são adquiridos e controles são testados e verificados;

(3) relatórios, emque os resultados da auditoria são organizados e apresentados.

Conclusão: o provedor de nuvem é seguro com a gestão de riscos e a gestão de segurança da informação, comum processo de melhoria contínua que culmina com a assertividade cada vez maior da visão de riscos e dos controles implantados.

Com a auditoria, assim, pode ser confirmada para a alta gestão da empresa que o negócio está funcionando bem e está preparado para enfrentar os potenciais desafios.

Controles Gerais de Auditoria de Sistemas

Controles de Segurança e Privacidade

Os controles podem ser físicos (como monitoramento de circuito fechado de TV, de acesso a data center), tecnológicos (como firewall, VPN) ou processuais (como atualização periódica de sistema operacional ou atualização das regras do firewall) e são aplicados nos ativos para que as vulnerabilidades sejam tratadas.

Os controles de segurança são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança.

Os controles de privacidade são salvaguardas administrativas, técnicas e físicas aplicadas em sistemas e organizações para gerenciar riscos de privacidade e para assegurar conformidade com requisitos de privacidade aplicáveis.

Os requisitos de segurança e privacidade direcionam a seleção e implementação de controles de segurança e privacidade e são derivados de leis, ordens executivas

Controles de Segurança e Privacidade

Diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas e transmitidas, e também para gerenciar riscos (NIST, 2020).

O NIST Cybersecurity Framework (NIST, 2018) define as cinco funções da segurança: identificação, proteção, detecção, resposta e recuperação.

Controles Organizacionais e relação com segurança e continuidade do Serviço

A segurança e privacidade fazem parte do contexto das empresas e estão integradas com outros assuntos, como a governança de TI.

A governança de TI visa a transformação digital e a relação com a entrega de valor, a mitigação dos riscos de negócios e a otimização de recursos.

A governança tem como principais objetivos (COBIT, 2018):

Avaliação de necessidades, condições e opções de todos os atores envolvidos, em busca de determinar objetivos corporativos balanceados.

Direcionamento para a priorização e tomada de decisão.

Monitoramento do desempenho e conformidade de acordo com os direcionamentos e objetivos definidos.

COBIT (Control Objectives for Information and RelatedTechnology)

O COBIT é um framework de governança de TI que trata de uma visão organizacional, a qual tem relação com a segurança e privacidade.

O COBIT define os componentes para construir e sustentar um sistema de governança, composto por processos, estrutura organizacional, políticas, procedimentos, fluxos de informação, cultura, comportamentos, qualificações e infraestrutura.

Há cinco domínios no COBIT, um para a governança e quatro para o gerenciamento (COBIT, 2018), sendo composto por um total de 40 processos, que podem ser entendidos como controles organizacionais.

Os exemplos citados dos 40 processos organizacionais são referentes aos controles de segurança:

Avaliar, direcionar e monitorar;

Alinhar, planejar e organizar;

Construir, adquirir e implementar;

Entregar serviço e suporte;

Monitorar, verificar e avaliar.

Alguns processos ou objetivos de controle organizacionais definidos no COBIT, estão voltados diretamente para a segurança. Por exemplo, a condução de auditorias do sistema de gestão da segurança da informação em intervalos definidos é uma das atividades que devem ser feitas (COBIT, 2018).

ITIL (Information Technology Infrastructure Library)

O ITIL é um framework de melhores práticas que visa auxiliar as empresas a entregar e suportar serviços de TI, provendo uma estrutura alinhada com a visão, missão, estratégia e objetivos da organização. Há um sistema de valor dos serviços, composto por : Cadeia de valor de serviços. Princípios. Governança. Melhoria contínua. 34 práticas de gerenciamento.

Dentre os benefícios do ITIL para as empresas, estão :

Padronização do modelo de operação de TI.

Cumprimento dos requisitos de clientes e funcionários.

Maior agilidade e capacidade para inovação.

Entregas em ambientes em constante mudança.

Maior controle e governança.

Demonstração do valor de TI.

Oportunidade para melhorias.

As 34 práticas do ITIL envolvem guias que são agrupadas em três categorias : Práticas de gerenciamento geral.

Práticas de gerenciamento de serviço.

Práticas de gerenciamento técnico.

Controles de Acesso possuem 4 categorias e suas subcategorias

Requisitos do negócio para controle de acesso.

1- Política de controle de acesso

2- Acesso às redes e aos serviços de rede

Gerenciamento de acesso de usuário

1- Registro e cancelamento de usuário

2- Provisionamento para acesso de usuário

3- Gerenciamento de direitos de acesso privilegiado

4- Gerenciamento de informação de autenticação secreta de usuário

5- Análise crítica dos direitos de acesso de usuário

6- Retirada ou ajuste de direitos de acesso

Responsabilidade dos usuários

1- Uso da informação de autenticação secreta

Controle de acesso ao sistema e a aplicação

1- Restrição de acesso à informação

2- Procedimentos seguros de entrada do sistema (log-on)

3- Sistema de gerenciamento de senha

4- Uso de programas utilitários privilegiados

5- Controle de acesso ao código-fonte de programas

Controles Lógico, Físico e Processual

Os controles de segurança envolvem investimentos em pessoas, processos e tecnologias, principalmente para o desenvolvimento de uma cultura de segurança, e podem ser administrativos, técnicos ou operacionais.

Alguns exemplos são (ISACA, 2017):

Conscientização.

Políticas.

Sistemas de detecção de intrusão.

Registro de eventos (logging).

Varredura de vulnerabilidades.

Classificação da informação.

Hardening de arquitetura e de tecnologia.

Hardening de sistemas.

Relatório do planejamento com foco nos controles

Tipos de controles considerados e para que servem:

Controles são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança, e também para assegurar conformidade com requisitos aplicáveis.

Os controles podem ser:

1- Técnicos, tecnológicos ou lógicos, como o antivírus ou o backup;

2- Processuais, administrativos ou operacionais, como a política de segurança ou o processo de revisão de contas de usuários;

3- Físicos, como o cadeado para que o desktop utilizado pelo presidente da empresa não seja roubado.

Como os controles são definidos: os controles são definidos **pelos riscos** existentes na empresa, que direciona mas necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos.

Além dos riscos, a definição dos controles pode ser feita a partir de requisitos que direcionam a seleção e implementação de controles, e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa.

Normas ou frameworks que podem ser a base para a definição dos controles: a ABNT NBR ISO/IEC 27002 define um conjunto de objetivos de controle de segurança da informação, e pode ser utilizada para a definição dos controles.

COBIT é um framework para governança de TI e possui um conjunto de controles mais amplos que podem ser implantados, incluindo os de segurança e privacidade.

ITIL é um conjunto de melhores práticas para o gerenciamento de serviços e estabelece também um conjunto de controles mais amplos que inclui aspectos de segurança.

Controles para aquisição, desenvolvimento e manutenção de sistemas: os controles para este assunto devem incluir os requisitos de segurança de sistemas de informação, para garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. É necessário ainda que controles de segurança sejam definidos em processos de desenvolvimento e de suporte, para garantir que a segurança da informação esteja projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. Os controles de segurança devem ainda abordar os dados para

teste, principalmente nos aspectos de privacidade, que devem ser reforçados devido à Lei Geral de Proteção de Dados Pessoais (LGPD).

Controle de acesso: o controle de acesso deve ser tratado pelos requisitos do negócio para controle de acesso, com a política de controle de acesso e o acesso às redes e aos serviços de rede.

O gerenciamento de acesso do usuário deve incluir aspectos como o registro e cancelamento de usuário, provisionamento para acesso de usuário, gerenciamento da informação de autenticação secreta de usuários e análise crítica dos direitos de acesso de usuário. O controle para as responsabilidades dos usuários deve envolver o uso da informação de autenticação secreta. O controle de acesso ao sistema e à aplicação deve envolver a restrição de acesso à informação, procedimentos seguros de entrada no sistema (log-on), uso de programas utilitários privilegiados e controle de acesso ao código-fonte de programas.

Auditoria: a auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados.

Técnicas e Ferramentas para Auditoria de Sistemas

Sua Missão visa 7 técnicas e ferramentas

A área segura.
Os racks com os servidores e os equipamentos de comunicação.
Os administradores de sistemas.
As máquinas virtuais.
Sistemas operacionais disponibilizados para os clientes.
Sistema de provisionamento de acesso aos clientes.

Você verá que a **auditoria requer um profissional com várias habilidades e competências, com uma visão abrangente**, para definir as técnicas e ferramentas necessárias para a auditoria e para utilizá-las no trabalho em campo. Uma empresa segura de fato precisa da auditoria, então a aplicação de todo o conhecimento é importante.

O objetivo e o escopo da auditoria podem estar relacionados com a conformidade com normas, padrões, frameworks, leis e requisitos de negócios.

A auditoria avalia e verifica a eficácia e eficiência dos controles implantados, que são necessários de acordo com a avaliação de riscos e das normas, padrões, frameworks, leis e requisitos de negócios relacionados.

Alguns exemplos de abordagens para as auditorias :

Governança
Riscos
Gestão
Processos de gestão de riscos.

Objetivos de Auditoria de Sistemas

Alguns exemplos de objetivos de auditoria para a segurança e privacidade das empresas, que exigem o planejamento de procedimentos, técnicas e ferramentas específicos, são (ISACA, 2017):

Políticas, padrões e procedimentos de segurança adequados e efetivos.

Riscos emergentes identificados, avaliados e tratados de uma forma confiável e adequada.

Ataques e brechas são identificados e tratados no tempo e na forma apropriados.

Principais Técnicas e Ferramentas para Auditoria de Sistemas

Auditoria de controles de segurança e privacidade exige um conjunto de habilidades que envolvem aspectos especializados, tais como para os pentests, a análise de configurações de servidores ou firewalls, ou revisão de regras de ferramentas de segurança (ISACA, 2017).

As auditorias são normalmente compostas por um conjunto de metodologias, técnicas e ferramentas.

Elas devem ser utilizadas para identificar, levantar evidências e para analisar e validar as evidências .Além disso, as metodologias, técnicas e ferramentas devem auxiliar o auditor a organizar e documentar os resultados. Há técnicas para interagir com as pessoas em busca das informações, que se complementam às análises manuais e às análises técnicas.

Objetivos das técnicas e ferramentas

Suas etapas são:

Identificar e levantar evidências

Analisar e validar as evidências

Organizar os resultados

As Técnicas e ferramentas envolvem:

Interação com as pessoas

Análise manual

Análise técnica com ferramentas

Dentre as técnicas e ferramentas que envolvem interação com pessoas, estão (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

Entrevistas

Questionários

Pesquisas

Perguntas e observação

Dinâmicas em grupo.

Já a análise manual pode ser feita com (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020)

Análise e revisão de documentação.

Análise de políticas, procedimentos e processos.

Análise de configurações.

Desenho de fluxos para documentar processos de negócios e controles automatizados.

Simulação de mesa.

Revisões gerenciais.

Autoavaliação.

Análise de código.

Objetivos das técnicas e ferramentas

A análise técnica com uso de ferramentas é um dos principais métodos que exige um conhecimento técnico amplo dos auditores e inclui :

Planilhas eletrônicas
Scripts
Software de auditoria Ferramentas de auditoria específicas
Software especializado - S.O, B.D, arquivos.
Logs de auditorias e relatórios
Simulações passo a passo
Execução de controles:
Metodologias para coleta de transações.
Pentests ou testes de penetração.

Aplicabilidade das técnicas e ferramentas para auditorias

O universo a ser avaliado em uma auditoria de segurança e privacidade pode ser baseado em três linhas de defesa, que direcionam como as técnicas e ferramentas podem ser aplicadas (ISACA, 2017):

Gestão interna
Gestão de riscos
Auditoria interna

A auditoria interna é essencial para a avaliação de desempenho do SGSI e é **bastante similar com a auditoria de certificação** (MCCREANOR, 2020):

Definição de escopo e levantamento de pré-auditoria;
Planejamento e preparação
Trabalho em campo
Análise
Reporte.

Relatório das técnicas e ferramentas que serão utilizadas na auditoria

Os controles implantados no data center foram resultados da avaliação de riscos, que direcionaram as necessidades com base na probabilidade das ameaças se tornarem incidentes de segurança e os impactos envolvidos.

Além dos riscos, a definição dos controles foi feita a partir de requisitos que direcionam a seleção e implementação de controles e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades da empresa, como a norma de certificação de data centers TIA-942, o padrão de segurança PCI DSS da indústria de cartões de pagamento e as melhores práticas de gerenciamento de serviços ITIL.

O primeiro ponto da auditoria é a realização de uma avaliação de riscos, para que todos os riscos do escopo referente ao datacenter tenham sido mapeados.

Na avaliação de riscos, devem ser identificados e mapeados ameaças, agentes de ameaças, ativos, suas vulnerabilidades, e calculados a probabilidade e os impactos.

Os ativos são:

A área segura.
Os racks com os servidores e os equipamentos de comunicação.
Os administradores de sistemas.
As máquinas virtuais.
Sistemas operacionais disponibilizados para os clientes.

Sistema de provisionamento de acesso aos clientes.

Após a avaliação dos riscos, o tratamento dos riscos pode se basear nos controles do TIA-942, PCI DSS, ABNT NBR ISO/IEC 27002, NIST Cybersecurity Framework, ITIL e COBIT, entre outros, focando nestes ativos. Os controles das diferentes normas, padrões e frameworks são equivalentes e complementares.

A verificação dos controles pode ser feita pensando nos controles técnicos, físicos e processuais, que são utilizados pela empresa.

Os principais controles existentes na empresa devem estar cumprindo os objetivos de, pelo menos:

Políticas de segurança da informação.

Organização da segurança da informação.

Segurança em recursos humanos.

Gestão de ativos.

Controle de acesso.

Criptografia.

Segurança física e do ambiente.

Segurança nas operações.

Segurança nas comunicações.

Aquisição, desenvolvimento e manutenção de sistemas.

As técnicas e ferramentas para a auditoria no provedor de nuvem podem incluir, pelo menos:

Análise das políticas, processos e procedimentos de segurança e privacidade.

Entrevistas com todas as áreas da empresa para percepção sobre se a política de segurança é de conhecimento organizacional e se está sendo seguida.

Visita ao data center para analisar a segurança física.

Análise de configuração do firewall.

Análise do fluxo para gestão de identidades.

Pentest para identificar vulnerabilidades do ambiente.

Análise de logs do banco de dados.

Análise dos relatórios do IDS/IPS.

Análise dos antivírus.

Teste de phishing.