Segurança e Auditoria de Sistemas

Política e Cultura de segurança

Profª. Ms. Adriane Ap. Loper

1

- Unidade de Ensino: 2
- Competência da Unidade: Conceitos de Políticas de segurança. Gerenciamento e aspectos operacionais da segurança de sistemas (éticos e legais).
- Resumo: Principais definições de cultura e políticas em segurança da inforamação.
- Palavras-chave: cultura, ética, política
- Título da Teleaula: Política e Cultura de segurança
- Teleaula nº: 2

2

Contextualização

- Uma empresa é composta por uma matriz em Natal- RN e filial em Belo Horizonte -MG.
- Com foco em energias renováveis, o desenvolvimento de novas tecnologias é feito por também por uma equipe que fica em Santiago, no Chile.
- Há laboratórios conectados em Belo Horizonte e Santiago. A empresa possui projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.
- A empresa possui um diretor de segurança da informação, que é o responsável por uma estrutura que inclui uma gerência de governança de segurança, uma gerência de

3

Contextualização

tecnologias de segurança e outra gerência de processos de segurança

- Você é o gerente de processos de segurança, e deve trabalhar em sinergia com os outros dois gerentes para alinhar os planos e atividades de segurança da informação da empresa.
- O diretor de segurança da informação da empresa solicitou um status dos aspectos normativos da empresa, e você deve preparar uma apresentação para reportar o status.
- É preciso um alinhamento com o gerente de governança de segurança e o gerente de tecnologias de segurança.

4

Contextualização

- Estruture uma apresentação descrevendo os tópicos com detalhes.
- Os tópicos a serem abordados são listados a seguir.
- Frameworks de segurança disponíveis e qual a empresa segue.
- Aspectos de negócios, legais, normativos e contratuais que devem ser considerados pela empresa.
- Controles de segurança da empresa: como são definidos, e quais são.
- Estrutura normativa, considerando políticas, normas, diretrizes, normas, procedimentos, guias.

5

Cybersecurity, CIS *Controls e* família NBR ISO/IEC 27.000

6

Contextualizando

- 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.

Fonte: Shutterstock

7

Contextualizando

- 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.

Fonte: Shutterstock

8

Contextualizando

- 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.

Fonte: Shutterstock

9

Cybersecurity Framework, do NIST

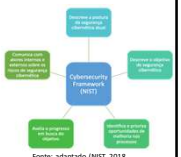
- O Cybersecurity Framework do National Institute of Standards and Technology (NIST) (NIST, 2018) organiza diferentes elementos da segurança da informação, focando no uso de direcionadores de negócios para guiar atividades de segurança cibernética, considerando os riscos de segurança da informação.

Fonte: adaptado (NIST, 2018)

10

Cybersecurity Framework, do NIST

- 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.



Fonte: adaptado (NIST, 2018

11

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 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).

Fonte: adaptado de (CIS, 2020).

12

Principais normas e padrões

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.

https://aws.amazon.com/pt/compliance/iso-27001-faqs

13

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.

https://aws.amazon.com/pt/compliance/iso-27001-faqs/

14

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.

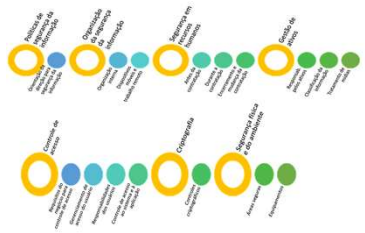
15

Objetivos de controles de segurança da informação da ABNT NBR ISO/IEC 27002

Fonte: adaptado de (ISO 27002, 2013).

16

Objetivos de controle e controles de segurança da informação da ABNT NBR ISO /IEC 27002.



17

ISO 27002

18

Ano: 2020 Banca: INSTITUTO AOCP Órgão: MJSP Prova: INSTITUTO AOCP - 2020 - MJSP - Analista de Governança de Dados - Big Data
Em uma situação na qual é necessário o acesso externo a informações, assinale a alternativa que apresenta uma recomendação da ISO 27002.

a) Limitar o acesso às informações antes da implantação dos controles apropriados.
b) Garantir o acesso às informações para avaliação das vulnerabilidades posteriores.
c) Permitir o acesso às informações dentro de um ambiente de testes.
d) Bloquear totalmente o acesso às informações antes da implantação dos controles apropriados.
e) Impor normas de acesso independentemente das particularidades de cada agente externo.

19

Ano: 2020 Banca: INSTITUTO AOCP Órgão: MJSP Prova: INSTITUTO AOCP - 2020 - MJSP - Analista de Governança de Dados - Big Data
Em uma situação na qual é necessário o acesso externo a informações, assinale a alternativa que apresenta uma recomendação da ISO 27002.

a) Limitar o acesso às informações antes da implantação dos controles apropriados.
b) Garantir o acesso às informações para avaliação das vulnerabilidades posteriores.
c) Permitir o acesso às informações dentro de um ambiente de testes.
d) Bloquear totalmente o acesso às informações antes da implantação dos controles apropriados.
e) Impor normas de acesso independentemente das particularidades de cada agente externo.

20

Sistema de Gestão de Segurança da Informação (SGSI)

21

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.


Fonte: Shutterstock

22

Sistema de Gestão de Segurança da Informação (SGSI)

- 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.


Fonte: Shutterstock

23

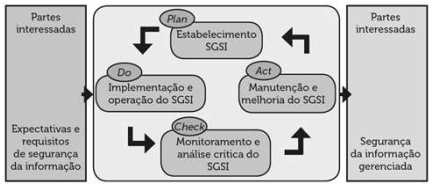
Sistema de Gestão de Segurança da Informação (SGSI)

- 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*.


Fonte: Shutterstock

24

SGSI - PDCA



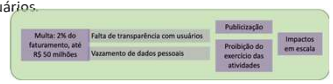
25

SGSI - Requisitos

26

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 a 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.



27

Lei Geral de Proteção de Dados Pessoais (LGPD)

- 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.

28

Marco Civil da Internet

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.

O Marco Civil da Internet trata de temas como neutralidade da rede, privacidade e retenção de dados, além de impor obrigações de responsabilidade civil aos usuários e provedores.

A lei ainda trata da confidencialidade das comunicações privadas, e dá especial atenção aos dados de registros de acesso, como endereços de IP e *logins*.

29

Lei Carolina Dieckmann

- 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.

30

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.

https://mscamposbr.wordpress.com/2018/06/14/comportamento-dos-funcionarios-compromete-seguranca-cibernetica/

31

Política de segurança da informação

A política de segurança é composta por um conjunto de documentos ou capítulos com regras, papeis e responsabilidades que devem ser lidos, compreendidos e seguidos pelos respectivos responsáveis.

32

Política de segurança da informação

Objetivos de uma política de segurança
A segurança é de responsabilidade de todos, e não apenas da área de segurança da empresa.
De fato, basta um incidente para que toda a empresa seja comprometida: vírus, vazamentos ou desenvolvimento de produtos vulneráveis que levam à má reputação (NAKAMURA; GEUS, 2007).

https://mscamposbr.wordpress.com/2018/06/14/comportamento-dos-funcionarios-compromete-seguranca-cibernetica/

Três estratégias básicas:
1. Termo assinado;
2. Campanhas e Tecnologias;
3. Treinamentos periódicos.

33

Apresentação

34

- A cultura de segurança da informação é feita por **todos** os funcionários da empresa.
- O primeiro passo é fazer com que a própria empresa queira buscar este fortalecimento da cultura. Para isto, você articula com a alta direção a revisão da política de segurança da empresa, e propõe um plano de comunicação que envolve a divulgação da nova versão da política de segurança, com a participação direta deles.
- O plano de comunicação envolve ainda treinamentos e campanhas de conscientização de cada uma das normas de segurança da empresa.

35

- Você irá perceber que o fortalecimento da cultura de segurança irá acontecer com a participação da alta direção, pois os funcionários sentirão que a segurança da informação é de fato algo importante, e todos estão trabalhando em prol deste objetivo.
- Você pode ainda propor que a empresa busque uma certificação de segurança da informação, justificando que a cultura de segurança da informação passa pela percepção também dos clientes e fornecedores.
- Cite os benefícios da certificação ISO 27001 e as principais características de um sistema de gestão de segurança da informação (SGSI).

36

Interação

37

Entenderam os aspectos não tecnológicos da Segurança da Informação?

Fonte: https://pixlr.com/en/X0L9

38

Cultura de segurança e privacidade

39

Contextualizando

- Estruture sua apresentação descrevendo os seguintes tópicos:

1. Cultura de segurança e privacidade.
2. Como a segurança é tratada pelos agentes externos.
3. Como a segurança é tratada para os usuários e para os administradores de sistemas.
4. Segurança no desenvolvimento de sistemas.

40

Cultura de segurança - definições

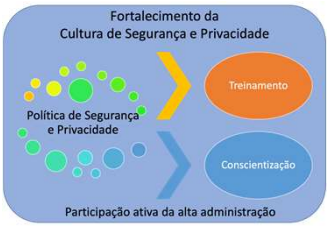
41

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 influencia 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.

41

Fortalecimento da cultura de segurança e privacidade.

42



Fonte: elaborado pelo autor

42

Política de Segurança e Privacidade

Fonte: elaborado pelo autor.

43

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.

44

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).

- Fonte: elaborado pelo autor.

45

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.

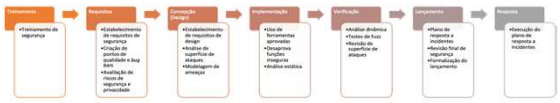
46

Análises de segurança em diferentes níveis

- O DAST também deve ser realizado antes do software entrar em produção, e o teste é 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).

47

Ciclo de vida de desenvolvimento seguro



Fonte: Adaptado de (LIPNER, 2010).

48

Relatório

49

1. Prepare um relatório indicando o ciclo de vida de desenvolvimento seguro de software adotado pela empresa, incluindo elementos como os requisitos de segurança desde a concepção, e testes de segurança de análise estática (SAST) e de análise dinâmica (DAST). Além disso, apresente a modelagem da superfície de ataques e de ameaças que foi considerado, justificando as medidas de segurança que estão sendo implementadas. Mostre que, antes do sistema ir para o ambiente de produção, estão previstos pentests.

50

Sobre o modelo de contratação de nuvem, mostre as responsabilidades de segurança envolvidos no IaaS e no PaaS.

Apresente as responsabilidades de sua equipe de segurança. Por fim, faça uma matriz de responsabilidades de sua equipe e dos provedores de nuvem, justificando as razões pela escolha pelo IaaS, contando com a sua equipe capacitada a executar as atividades necessárias de segurança.

51

Armazenamento de dados

52

Contextualizando

Sua missão:
Estruture sua apresentação com os seguintes tópicos:
1.Tratamento de dados pessoais
2.Controles de segurança para proteção dos dados pessoais
3.Uso de provedores de nuvem

53

Contextualizando

- 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.

54

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.

55

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

- 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.

56

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).

57

Mascaramento, anonimização e pseudonimização

- 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.

58

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).

59

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.

60

Relatório

61

- Sua empresa deverá coletar dados pessoais, incluindo o nome completo, CPF endereço e referência comercial.
- O termo de privacidade deve citar quais são os dados que estão sendo coletados, descrevendo claramente a finalidade, e como eles estarão protegidos, citando ainda os provedores de serviços, se estiver sendo utilizados.
- Você deve definir também se estes dados serão compartilhados com algum terceiro, se caso afirmativo, deve obter um consentimento de cada usuário.
- Para o armazenamento dos dados coletados, você deve pensar nos mecanismos de proteção. Além dos controles de segurança para proteger os ativos físicos e lógicos, os dados podem ser pseudonimizados.

62

- Assim, você pode utilizar um código como "Cliente0001" para o João, "Cliente0002" para Maria, e assim por diante.
- No banco de dados, você pode armazenar este código do cliente como identificador, juntamente com os dados de CPF, endereço e referência comercial.
- Este relacionamento entre o código do cliente e o nome real também deve ser armazenado, de uma forma segura e em local distinto da base de dados dos clientes.
- Para aumentar a segurança, você pode dividir ainda mais o banco de dados, com o CPF em um, e o endereço e referência comercial em outro, usando o código do cliente como identificador.

63

- A anonimização não pode ser aplicada no seu caso, pois você precisa identificar o cliente.
- Ela pode, no entanto, ser utilizada para criar uma base distinta para inteligência de negócios, por exemplo.
- Outro ponto que você deve definir é como a criptografia irá funcionar, se na aplicação ou no banco de dados.
- Outro ponto está relacionado às responsabilidades de segurança, de acordo com o tipo de serviço contratado do provedor de nuvem. H
- á as modalidades de contratação de infraestrutura, plataforma ou o serviço.

64

Interação

65

Entenderam a complexidade dos aspectos de segurança da informação?

Fonte: https://gifer.com/en/XOL9

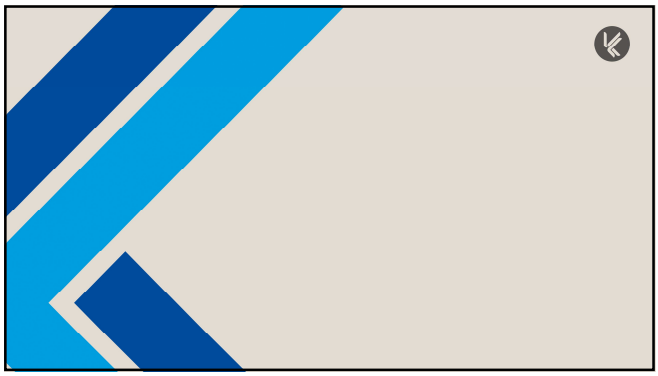
66

Recapitulando

67

- ✓ Política e Cultura de segurança
- ✓ Gestão e Políticas de segurança
- ✓ Cultura de Segurança
- ✓ Armazenamento de Dados

68



69