SIMULADO SOMATIVO

BACHARELADO EM SISTEMAS DA INFORMAÇÃO
DISCIPLINA: SEGURANÇA EM INFORMÁTICA
PROFESSOR (A): PEDRO GRESS
ALUNO (A):Luan Brito Sousa Calazans
E-MAIL:calazanscybersec@gmail.com
Valor: 1,5 **ponto**

CADERNO DE QUESTÕES

1)

Durante uma reunião da equipe técnica da empresa *Delta Farma Digital*, especializada em prontuários eletrônicos, um analista júnior questionou o significado exato do termo **vulnerabilidade**, após o relatório de avaliação de riscos apontar que “vulnerabilidades críticas em endpoints expõem a rede corporativa a ataques de ransomware”.

Um dos gerentes pediu que cada membro da equipe explicasse com suas palavras o que entendia por **vulnerabilidade**, com o objetivo de nivelar o vocabulário técnico entre os setores.

Considerando os fundamentos da segurança da informação, **qual das definições a seguir mais se alinha ao conceito técnico de vulnerabilidade**?

1) **É uma falha ou** fraqueza **que pode ser explorada por uma ameaça para causar dano.**

2)

Durante um treinamento interno de segurança da informação em uma empresa de software, o instrutor apresentou quatro situações relacionadas a ataques que comprometem as propriedades fundamentais da informação: **confidencialidade, integridade, disponibilidade e autenticidade**.

O objetivo era identificar corretamente o tipo de ataque associado a cada situação, com base nas definições adotadas em frameworks como ISO/IEC 27001

e RFC 4949.

Situações apresentadas

9) Um disco rígido é fisicamente destruído após uma sabotagem interna.

35) Arquivos confidenciais são copiados por um usuário sem autorização.

61) Um funcionário malicioso altera dados de salário em uma planilha protegida. **IV)** Um script automatizado insere registros falsos em um banco de dados de logs.

Associe cada situação ao respectivo tipo de ataque abaixo:

1. Interrupção
2. Interceptação
3. Modificação
4. Fabricação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:

1) **I–1 II–2 III–3 IV–4**

disponibilidade e autenticidade.

O objetivo era identificar corretamente o tipo de ataque associado a cada situação, com base nas definições adotadas em frameworks como ISO/IEC

---

3)

Durante um treinamento interno de segurança da informação em uma empresa de software, o instrutor apresentou quatro situações relacionadas a ataques que comprometem as propriedades fundamentais da informação: **confidencialidade, integridade,**

27001 e RFC 4949.

Situações apresentadas

9) Um disco rígido é fisicamente destruído após uma sabotagem interna.

35) Arquivos confidenciais são copiados por um usuário sem autorização.

61) Um funcionário malicioso altera dados de salário em uma planilha protegida.

IV) Um script automatizado insere registros falsos em um banco de dados de logs.

Associe cada situação ao respectivo tipo de ataque abaixo:

1. Interrupção
2. Interceptação
3. Modificação
4. Fabricação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:

1) **I–4 II–3 III–2 IV–1**

---

4)

Durante um treinamento interno de segurança da informação em uma empresa de software, o instrutor apresentou quatro situações relacionadas a ataques que comprometem as propriedades fundamentais da informação: **confidencialidade, integridade, disponibilidade e autenticidade**.

O objetivo era identificar corretamente o tipo de ataque associado a cada situação, com base nas definições adotadas em frameworks como ISO/IEC 27001 e RFC 4949.

Situações apresentadas

9) Um disco rígido é fisicamente destruído após uma sabotagem interna.

35) Arquivos confidenciais são copiados por um usuário sem autorização.

61) Um funcionário malicioso altera dados de salário em uma planilha protegida.

IV) Um script automatizado insere registros falsos em um banco de dados de logs.

Associe cada situação ao respectivo tipo de ataque abaixo:

1. Interrupção
2. Interceptação
3. Modificação
4. Fabricação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:

1) **I–4 II–3 III–2 IV–1**

---

5)

Durante um treinamento interno de segurança da informação em uma empresa de software, o instrutor apresentou quatro situações relacionadas a ataques que comprometem as propriedades fundamentais da informação: **confidencialidade, integridade, disponibilidade e autenticidade**.

O objetivo era identificar corretamente o tipo de ataque associado a cada situação, com base nas definições adotadas em frameworks como ISO/IEC 27001 e RFC 4949.

Situações apresentadas

9) Um disco rígido é fisicamente destruído após uma sabotagem interna.

35) Arquivos confidenciais são copiados por um usuário sem autorização.

61) Um funcionário malicioso altera dados de salário em uma planilha protegida.

IV) Um script automatizado insere registros falsos em um banco de dados de logs.

Associe cada situação ao respectivo tipo de ataque abaixo:

1. Interrupção
2. Interceptação

3. Modificação
4. Fabricação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:

1) **I–4 II–3 III–2 IV–1**

---

6)

Um influenciador digital publica em uma rede social conteúdo ofensivo e difamatório contra uma empresa, resultando em danos à sua reputação. A empresa, sentindo-se prejudicada, envia uma notificação extrajudicial diretamente ao provedor da rede social solicitando a remoção imediata do conteúdo. O provedor, contudo, mantém a publicação no ar, alegando que só pode agir mediante ordem judicial.

Posteriormente, o caso chega ao Poder Judiciário, que determina a remoção do conteúdo. Durante o processo, discute-se se o provedor deveria ter sido responsabilizado desde a notificação inicial da empresa, sem necessidade de ordem judicial.

Com base no artigo 19 do Marco Civil da Internet e na jurisprudência do STF:

1) **O provedor só poderia ser responsabilizado se descumprisse ordem judicial, exceto em situações de flagrante violação de direitos de difícil reversão, como conteúdo de ódio ou ilícito evidente.**

---

7)

A gestão de riscos em segurança da informação consiste em um conjunto de processos sistemáticos para identificar, analisar, avaliar e tratar riscos que possam comprometer ativos críticos da organização. Normas como a ISO 31000 e a ISO 27005 fornecem diretrizes para estruturar essa prática, utilizando escalas de probabilidade e impacto para priorização e tomada de decisão. Entretanto, a eficácia do processo depende também de fatores humanos, como a cultura organizacional, a conscientização dos colaboradores e a comunicação interna, que garantem a correta percepção dos riscos e o engajamento na aplicação de medidas preventivas e corretivas.

De acordo com as boas práticas de gestão de riscos em segurança da informação, qual das alternativas abaixo apresenta, simultaneamente, um elemento de caráter técnico e um elemento de caráter organizacional essenciais para a eficácia do processo?

1) **Aplicação de escalas de probabilidade x impacto e promoção de uma cultura de segurança entre os colaboradores.**

---

8)

Uma empresa de comércio eletrônico decidiu revisar seu processo de gestão de riscos de acordo com as diretrizes da ISO 31000 e ISO 27005. Durante a análise, a equipe de segurança identificou quatro situações envolvendo diferentes estratégias de tratamento de risco.

Situações apresentadas:

9) Implementação de autenticação multifator para reduzir a probabilidade de acesso não autorizado.

35)Contratação de seguro cibernético para cobrir perdas financeiras decorrentes

de incidentes.
61) Decisão de encerrar um serviço online que apresentava alto risco de exploração e custo elevado de mitigação.
IV) Manutenção de um risco classificado como baixo devido ao alto custo de controles em relação ao impacto esperado.

Associe cada situação à respectiva estratégia de tratamento de risco:

1. Redução
2. Transferência
3. Evitação
4. Aceitação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:
1) **I–1 II–2 III–3 IV–4**

---

9)

Uma empresa de comércio eletrônico decidiu revisar seu processo de gestão de riscos de acordo com as diretrizes da ISO 31000 e ISO 27005. Durante a análise, a equipe de segurança identificou quatro situações envolvendo diferentes estratégias de tratamento de risco.

Situações apresentadas:
9) Implementação de autenticação multifator para reduzir a probabilidade de acesso não autorizado.
35)Contratação de seguro cibernético para cobrir perdas financeiras decorrentes de incidentes.
61) Decisão de encerrar um serviço online que apresentava alto risco de exploração e custo elevado de mitigação.
IV) Manutenção de um risco classificado como baixo devido ao alto custo de controles em relação ao impacto esperado.

Associe cada situação à respectiva estratégia de tratamento de risco:

1. Redução
2. Transferência
3. Evitação
4. Aceitação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:

1) **I–1 II–2 III–3 IV–4**

---

10)

Uma instituição financeira, após um processo completo de gestão de riscos baseado na ISO 31000 e ISO 27005, implementou um conjunto de controles técnicos, físicos e administrativos para reduzir a probabilidade de ataques cibernéticos a seus sistemas de transações. Entre as medidas aplicadas estavam: autenticação multifator, criptografia de dados em repouso e em trânsito, monitoramento contínuo por SIEM e auditorias internas periódicas.

Mesmo após a adoção dessas medidas, a equipe de segurança identificou que certos cenários de ataque ainda poderiam ocorrer, embora com probabilidade reduzida, como tentativas sofisticadas de spear phishing direcionadas a executivos e vulnerabilidades zero-day não corrigidas imediatamente. Esse conjunto de riscos que permanece após a aplicação de controles foi registrado no relatório final como parte do processo de gestão.

No comitê de governança, surgiu um debate sobre a natureza desses riscos e sobre como avaliar a real eficácia das medidas adotadas, considerando o custo de implementação, o nível de exposição remanescente e a necessidade de planos de contingência.

Analise as asserções a seguir:

I – O risco residual corresponde ao nível de risco que permanece após a aplicação de medidas de tratamento, devendo ser monitorado e, quando necessário, mitigado com controles adicionais ou planos de contingência.

PORQUE

35– A avaliação da eficácia de controles considera não apenas a redução da probabilidade e do impacto dos riscos, mas também o custo-benefício das medidas implementadas em relação à exposição residual.

1) **As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.**

---

11)

A gestão de riscos em segurança da informação envolve a identificação, análise, avaliação e tratamento de riscos que possam comprometer a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade dos ativos organizacionais. A **matriz de riscos** é uma ferramenta essencial nesse processo, permitindo cruzar a probabilidade de ocorrência de um evento com o impacto potencial, facilitando a priorização das ações de mitigação.

Normas como a ABNT NBR ISO/IEC 27005 fornecem diretrizes para o uso da matriz de riscos, descrevendo metodologias para estimativa, categorização e decisão sobre o tratamento adequado. O correto entendimento de como utilizar essa ferramenta é fundamental para que as organizações otimizem recursos e mantenham a resiliência operacional.

Considerando o uso da matriz de riscos e sua aplicação na gestão de segurança da informação, assinale a alternativa que apresenta corretamente os conceitos e aplicações relacionados:

1) **A matriz de riscos cruza probabilidade e impacto, permitindo classificar riscos em níveis como baixo, médio e alto para orientar decisões de tratamento.**

pois representam menor custo de mitigação.

5) A matriz de riscos substitui integralmente outras ferramentas de gestão, tornando desnecessária a análise qualitativa ou quantitativa.

---

12)

A empresa *AgroVet Digital Ltda.*, localizada no interior de Goiás, é uma PME do setor agropecuário que recentemente contratou uma consultoria em cibersegurança para implementar um Sistema de Gestão de Segurança da Informação (SGSI), com base na norma **ISO/IEC 27001**.
Durante a auditoria interna realizada pela consultoria S17 CyberSec, foram detectadas as seguintes situações:

1. A empresa não possui um inventário formal de ativos da informação.
2. A análise de riscos foi feita sem a participação da alta direção.
3. Alguns controles recomendados no Anexo A da ISO/IEC 27001 foram aplicados mesmo sem relação direta com os riscos identificados.
4. Não há evidência de ações corretivas após os incidentes de 2023, embora estes tenham sido registrados informalmente em e-mails.
   O relatório de auditoria recomenda que a empresa reestruture seu SGSI para estar em conformidade com os princípios da norma, com foco no alinhamento estratégico e na melhoria contínua.

Considerando a norma ISO/IEC 27001 e as boas práticas de gestão de segurança da informação, qual das ações a seguir **é mais coerente** com a implementação eficaz de um SGSI nessa organização?

1) **Desenvolver o inventário de ativos e realizar nova análise de riscos com envolvimento da alta direção, visando à definição de controles proporcionais.**

---

13)

A empresa *AgroVet Digital Ltda.*, localizada no interior de Goiás, é uma PME do setor agropecuário que recentemente contratou uma consultoria em cibersegurança para implementar um Sistema de Gestão de Segurança da Informação (SGSI), com base na norma **ISO/IEC 27001**.
Durante a auditoria interna realizada pela consultoria S17 CyberSec, foram detectadas as seguintes situações:

1. A empresa não possui um inventário formal de ativos da informação.
2. A análise de riscos foi feita sem a participação da alta direção.
3. Alguns controles recomendados no Anexo A da ISO/IEC 27001 foram aplicados mesmo sem relação direta com os riscos identificados.
4. Não há evidência de ações corretivas após os incidentes de 2023, embora estes tenham sido registrados informalmente em e-mails.
   O relatório de auditoria recomenda que a empresa reestruture seu SGSI para estar em conformidade com os princípios da norma, com foco no alinhamento estratégico e na melhoria contínua.

Considerando a norma ISO/IEC 27001 e as boas práticas de gestão de segurança da informação, qual das ações a seguir **é mais coerente** com a implementação eficaz de um SGSI nessa organização?

1) **Desenvolver o inventário de ativos e realizar nova análise de riscos com envolvimento da alta direção, visando à definição de controles proporcionais.**

---

14)

Em 2023, a empresa MedConta Cloud S.A., especializada em soluções de gestão hospitalar, passou a ser investigada pela ANPD após uma denúncia de
vazamento de dados sensíveis. A organização possuía um SGSI certificado na norma ISO/IEC 27001, mas não havia feito mapeamento de dados pessoais, nem implementado políticas específicas de consentimento, revogação e direito ao esquecimento. Durante a análise de conformidade, a auditoria concluiu que a organização atendia requisitos técnicos de segurança da informação, mas não possuía mecanismos de governança específicos exigidos pela LGPD, como o Registro de Operações de Tratamento (ROPA) e o Relatório de

Impacto à Proteção de Dados Pessoais (RIPD).

Em relação à implementação da ISO/IEC 27001 e ao cumprimento da Lei Geral de Proteção de Dados (LGPD), analise as asserções a seguir:

I – A norma ISO/IEC 27001 contribui significativamente para a segurança técnica dos dados pessoais tratados por uma organização.

PORQUE

35– A ISO/IEC 27001, por si só, garante total conformidade jurídica com a LGPD, dispensando medidas específicas de governança de dados pessoais.

1) **A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.**

auditoria concluiu que a organização atendia requisitos técnicos de segurança da informação, mas não possuía mecanismos de governança específicos exigidos pela LGPD, como o Registro

---

15)

Em 2023, a empresa MedConta Cloud S.A., especializada em soluções de gestão hospitalar, passou a ser investigada pela ANPD após uma denúncia de vazamento de dados sensíveis. A organização possuía um SGSI certificado na norma ISO/IEC 27001, mas não havia feito mapeamento de dados pessoais, nem implementado políticas específicas de consentimento, revogação e direito ao esquecimento.

Durante a análise de conformidade, a

de Operações de Tratamento (ROPA) e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Em relação à implementação da ISO/IEC 27001 e ao cumprimento da Lei Geral de Proteção de Dados (LGPD), analise as asserções a seguir:

I – A norma ISO/IEC 27001 contribui significativamente para a segurança técnica dos dados pessoais tratados por uma organização.
PORQUE
35– A ISO/IEC 27001, por si só, garante total conformidade jurídica com a LGPD, dispensando medidas específicas de governança de dados pessoais.

1) **A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.**

---

16)

Para avaliar a real exposição a riscos, organizações precisam determinar o valor que seus dados possuem para o negócio. Essa avaliação é fundamental tanto para definir medidas de segurança quanto para apoiar decisões como a contratação de seguros. O valor do dado, nesse contexto, está relacionado a fatores como sua utilização nos processos de negócio, sua indispensabilidade, seu conteúdo e o grau de recuperação em caso de perda.

Qual fator não é importante para determinar o valor do dado para uma organização?

1) **O grau em que o dado faltante, incompleto ou incorreto pode ser recuperado.**

---

17)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) prevê obrigações de segurança no tratamento de dados pessoais e estabelece regras para a comunicação de incidentes de segurança. Analise as afirmativas a seguir:

I. O controlador e o operador devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, como destruição, perda ou alteração.

35. O controlador é obrigado a comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, informando ao menos a descrição da natureza dos dados

afetados.
III. O operador responde solidariamente com o controlador em qualquer incidente de segurança, ainda que não tenha descumprido instruções ou agido com culpa.
IV. A ausência de comunicação do incidente de segurança pela empresa pode gerar sanções administrativas previstas na LGPD, como advertência e multa, independentemente de outras esferas de responsabilização.

Está correto apenas o que se afirma em:

1) **I, II e IV.**

---

18)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) prevê obrigações de segurança no tratamento de dados pessoais e estabelece regras para a comunicação de incidentes de segurança. Analise as afirmativas a seguir:

I. O controlador e o operador devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, como destruição, perda ou alteração.
35. O controlador é obrigado a comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, informando ao menos a descrição da natureza dos dados afetados.

61. O operador responde solidariamente com o controlador em qualquer incidente de segurança, ainda que não tenha descumprido instruções ou agido com culpa.
IV. A ausência de comunicação do incidente de segurança pela empresa pode gerar sanções administrativas previstas na LGPD, como advertência e multa, independentemente de outras esferas de responsabilização.

Está correto apenas o que se afirma em:

1) **I, II e IV.**

---

19)

Em uma filial da empresa XPTO ocorreu um incêndio de grandes proporções. O corpo de bombeiros conseguiu conter as chamas antes que todo o prédio fosse comprometido, mas parte significativa dos servidores e documentos físicos foi perdida. As fitas de backup armazenadas em uma sala adjacente também foram danificadas pelo calor. Além disso, relatórios apontaram que alguns danos adicionais foram causados pela água e pelos produtos químicos utilizados pelos extintores durante o combate ao fogo. No relatório final, a equipe de segurança da informação precisou distinguir entre danos diretos
e danos indiretos decorrentes do incidente.

Qual dos seguintes exemplos corresponde a um **dano indireto** causado pelo incêndio na filial da empresa XPTO?

1) **provocados pela água e produtos químicos utilizados no combate ao incêndio.**

---

20)

Uma pequena empresa de tecnologia iniciou suas atividades com apenas um colaborador, mas após alguns anos expandiu para 20 funcionários e passou a lidar com um volume crescente de dados críticos. O gestor percebeu que já não era mais possível manter o controle de riscos de forma intuitiva e, por recomendação de um consultor, optou por iniciar um processo de análise qualitativa de riscos. Esse tipo de análise é frequentemente utilizado em empresas em crescimento, por fornecer uma visão inicial das ameaças mais relevantes de forma acessível, sem demandar dados estatísticos detalhados.

I. A análise qualitativa de riscos busca a classificação de ameaças e

vulnerabilidades usando como subterfúgio cenários e percepções, permitindo ao tomador de decisão priorizar riscos de forma subjetiva, mas prática.

PORQUE

35.A análise qualitativa de riscos utiliza cálculos estatísticos precisos e dados quantitativos para mensurar o impacto no capital da empresa visando o montante exato de cada risco identificado.

A respeito dessas asserções, assinale a opção correta:

1) **A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.**

---

21)

Durante um treinamento interno de segurança da informação em uma empresa de software, o instrutor apresentou quatro situações relacionadas a ataques que comprometem as propriedades fundamentais da informação: confidencialidade, integridade, disponibilidade e autenticidade.

O objetivo era identificar corretamente o tipo de ataque associado a cada situação, com base nas definições adotadas em frameworks como ISO/IEC 27001 e RFC 4949.

Situações apresentadas

9) Um disco rígido é fisicamente destruído após uma sabotagem interna.

35) Arquivos confidenciais são copiados por um usuário sem autorização.

61) Um funcionário malicioso altera dados de salário em uma planilha protegida.

IV) Um script automatizado insere registros falsos em um banco de dados de logs.

Associe cada situação ao respectivo tipo de ataque abaixo:

1. Interrupção
2. Interceptação
3. Modificação
4. Fabricação

Em seguida, assinale a alternativa que apresenta a sequência correta de associação:

1) **I–1 II–2 III–3 IV–4**

2)

---

22)

Durante a construção de uma política de segurança da informação, uma organização buscou garantir que os dados mantidos em seus sistemas fossem confiáveis tanto em sua origem quanto em seu conteúdo. A equipe de segurança decidiu implementar assinaturas digitais em comunicações e arquivos críticos, buscando preservar propriedades fundamentais como autenticidade e integridade da informação.

Contudo, parte da equipe demonstrou dúvidas sobre a diferença entre os dois conceitos e como se relacionam na prática da proteção de dados.

Analise as asserções a seguir:

I – A integridade da informação é garantida quando se assegura que os dados não foram alterados de forma indevida, intencional ou acidental.
PORQUE

35– A autenticidade da informação garante que os dados tenham origem legítima e possam ser atribuídos com confiança a uma fonte identificável.

1) **As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I.**

---

25)

Em um corredor de acesso livre dentro de uma empresa, encontra-se instalada uma impressora de rede multifuncional, utilizada por diversos setores. O equipamento não possui controle de autenticação, permitindo que qualquer colaborador ou visitante imprima, copie ou digitalize documentos sem registro de uso. Em auditoria, constatou-se que contratos e relatórios confidenciais foram esquecidos na bandeja da impressora, ficando expostos a pessoas não autorizadas.

Considerando o cenário descrito, discorra sobre os riscos de segurança da informação associados à situação, identificando:

1. Quais princípios da tríade CIA (Confidencialidade, Integridade, Disponibilidade) são afetados;
2. Quais vulnerabilidades e falhas de controles podem ser observadas;
3. Que medidas técnicas e administrativas poderiam ser implementadas para mitigar esses riscos.
   R: Essa situação afeta principalmente a integridade e confidencialidade dos dados sensíveis expostos, sendo possível que alguém mal-intencionado possa copiar as informações ou alterá-las, obtendo essas informações confidenciais para exploração e afins. Seria interessante adicionar um departamento de impressão, com uma pessoa de confiança para direcioná-lo, ou então colocar uma sala com controle de acesso, utilizando cartões ou chaves de acesso.
4.

---

24)

A segurança da informação estabelece um conjunto de práticas, políticas e controles voltados à proteção dos dados e sistemas organizacionais, garantindo os princípios de confidencialidade, integridade e disponibilidade. Dentro desse

contexto, é fundamental adotar uma linguagem comum que permita a comunicação clara entre gestores, técnicos e demais profissionais. Assim, conceitos como incidente de segurança, ativos, ameaças, vulnerabilidades,

riscos, ataques e impactos são estruturados de forma padronizada para orientar decisões estratégicas e técnicas. A definição precisa desses termos possibilita que todos os envolvidos em um processo de segurança compreendam de maneira uniforme as situações enfrentadas, auxiliando tanto na prevenção quanto na resposta a eventos adversos.

Com base nos fundamentos da segurança da informação e considerando a necessidade de uma linguagem comum entre profissionais de diferentes áreas, defina de forma objetiva:

1) Segurança da informação;
   É como um dado é tratado; no caminho do remetente ao receptor, não pode haver nenhum tipo de interferência. O dado deve ser entregue por uma pessoa de confiança, não pode ser modificado no meio do trajeto nem desviado de sua rota para evitar que seja copiado, e deve ser entregue diretamente nas mãos do receptor.
2) Incidente de segurança;
   Uma pessoa esta fazendo uma caminhada ela vê um qr code aleatorio em um local escondido na praia , ela fica curiosa e escaneia o qr code.
3) Ativo;
   Um ativo é qualquer recurso valioso para a organização, que pode incluir dados, sistemas, equipamentos, pessoas e processos. Ou seja ate mesmo acesso a cameras
4) Ameaça;
   Uma ameaça é qualquer evento ou ação que tenha o potencial de explorar uma vulnerabilidade e causar dano a um ativo.
5) Vulnerabilidade;
   É uma falha que existe nos sistemas devido à falta de atualização ou outros fatores. Essas vulnerabilidades, quando exploradas, "cospem" informações confidenciais sobre o sistema ou banco de dados. Ou podem ate dar acessoa a codigos remotos.
6) Risco;
   O risco acho que seria as coisas integras que você poderia perder ou até mesmo o risco de ser exposto com arquivos sensiveis ,ou dados criptografados prejudicando assim sua empresa e valores economicos
7) Ataque;
   Um ataque ocorre quando, de alguma maneira, alguém com más intenções consegue informações sobre coisas que não deveria ter, explorando desde vulnerabilidades de um sistema até vulnerabilidades humanas, como o amor, ou por meio de formas intimidadoras.
8) Impacto.

O impacto é o efeito que um incidente de segurança pode causar em uma

organização. Sendo um impacto economico

25)

A **Lei Geral de Proteção de Dados Pessoais (LGPD)**, sancionada no Brasil em 2018 e em vigor desde 2020, foi amplamente inspirada no **Regulamento Geral sobre a Proteção de Dados (GDPR/RGPD)** da União Europeia, adotado em 2016. Ambas legislações compartilham princípios fundamentais como: finalidade, adequação, necessidade, segurança, transparência e responsabilização.

Contudo, existem **diferenças significativas** entre os dois marcos. Por exemplo, enquanto o GDPR impõe a obrigatoriedade do **relatório de impacto à proteção de dados (DPIA)** em diversos cenários, a LGPD apenas **recomenda** esse instrumento. Além disso, o GDPR exige que a **nomeação do Data Protection Officer (DPO)** ocorra em uma gama maior de situações, incluindo controladores e operadores de órgãos públicos, enquanto a LGPD permite mais flexibilidade.

Ambas as normas reconhecem os direitos dos titulares e preveem sanções em caso de descumprimento, mas o GDPR permite multas mais severas e

imediatas, enquanto a LGPD dá margem para processos sancionatórios mais graduais conduzidos pela ANPD.

Com base na LGPD brasileira e no GDPR europeu, redija um texto explicando:

1) Duas semelhanças fundamentais entre LGPD e GDPR, no que tange à governança e aos direitos do titular.
2) Duas diferenças práticas que impactam diretamente a atuação do DPO em empresas multinacionais.
3) Um risco comum a ser mitigado por meio de controles técnicos do SGSI, conforme recomendações da ISO/IEC 27001.

(Limite: 15 linhas – Valor: 10,0 pontos)

Tanto a LGPD quanto o GDPR compartilham a base de princípios de governança como transparência, finalidade e responsabilização (accountability), exigindo que organizações demonstrem conformidade de forma proativa. Além disso, ambas garantem direitos amplos aos titulares, como acesso, retificação, portabilidade e exclusão de seus dados, empoderando os cidadãos no controle de suas informações.

Duas diferenças práticas impactam o DPO em multinacionais: a obrigatoriedade de nomeação é mais restrita na LGPD, aplicando-se principalmente a controladores de grande porte, enquanto no GDPR é exigida em mais cenários, incluindo operações públicas ou de monitoramento em larga escala. Outra diferença é o Relatório de Impacto (DPIA/RIPD), obrigatório no GDPR sob certas condições, mas apenas recomendado pela LGPD, o que exige do DPO uma adaptação de processos conforme a jurisdição.

Um risco comum a ambas as leis é o vazamento não autorizado de dados pessoais. Controles técnicos do SGSI baseados na ISO 27001, como criptografia, controle de acesso e monitoramento contínuo, são essenciais para mitigar esse risco, assegurando a confidencialidade e integridade das informações.

26)

Uma operadora de serviços digitais que atende em todo o território nacional registrou, no último trimestre, os seguintes incidentes de segurança:

- Incidente A: 250.000 contas de usuários tiveram senhas expostas por falha de configuração de banco de dados.
- Incidente B: 1.200 contas sofreram acessos não autorizados por ataque de força bruta, com uso fraudulento de dados de pagamento.
- Incidente C: 50.000 registros de clientes, contendo dados cadastrais, foram apagados indevidamente por erro de rotina de backup.

A empresa comunicou publicamente apenas o Incidente B, alegando que os outros não representariam risco ou dano relevante. Além disso, deixou de apresentar relatórios técnicos solicitados pelo Ministério Público e pela ANPD, sustentando que somente cumpriria determinação expressa do Poder Judiciário.

Com base na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e no Marco Civil da Internet (Lei nº 12.965/2014), responda de forma fundamentada:

Quais dos incidentes exigem comunicação obrigatória à ANPD e aos titulares, justificando sua resposta à luz do critério de "risco ou dano relevante" (art. 48 da LGPD). E que tipo de sanções administrativas e responsabilizações civis podem recair sobre a empresa pela omissão ou pela recusa em cooperar com autoridades competentes.

No caso do Incidente A (vazamento de senhas), é obrigatório comunicar à ANPD e aos titulares, pois há risco de uso indevido dos dados expostos. O Incidente B (acesso fraudulento a contas) também exige comunicação, pois envolve dados financeiros e riscos significativos para os titulares. Já o Incidente C (apagamento de dados) não exige comunicação obrigatória, pois não houve exposição ou roubo de informações. Se a empresa não comunicar ou cooperar com a ANPD, pode sofrer multas e responsabilidade civil, além de danos à sua reputação e à confiança dos clientes.