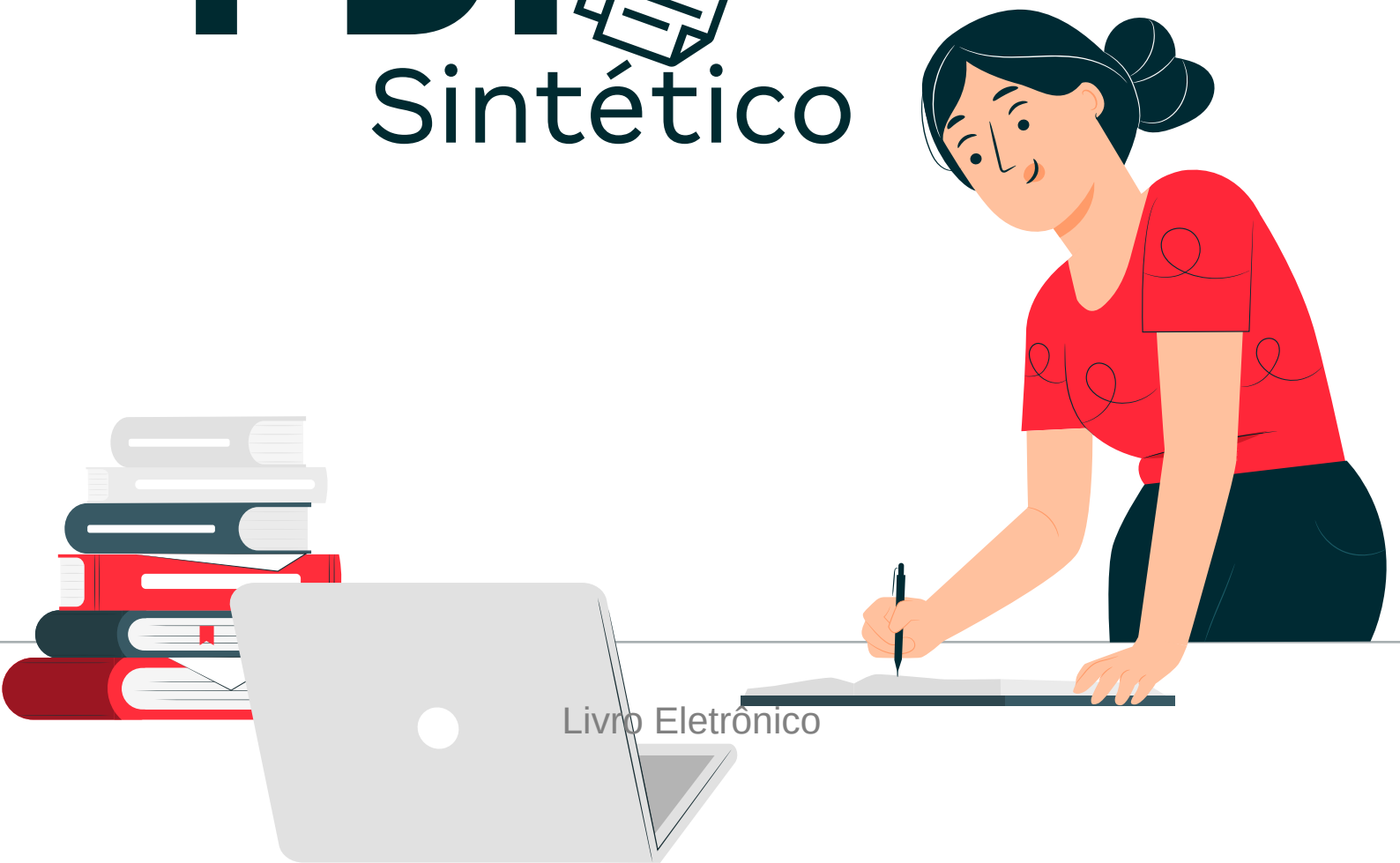
GRAN CONCURSOS

TECNOLOGIA DA INFORMAÇÃO - SEGURANÇA DA INFORMAÇÃO E LGPD

Apresentação e Propriedades Fundamentais

PDF Sintético



Livro Eletrônico

Presidente: Gabriel Granjeiro

Vice-Presidente: Rodrigo Calado

Diretor Pedagógico: Erico Teixeira

Diretora de Produção Educacional: Vivian Higashi

Gerência de Produção de Conteúdo: Magno Coimbra

Coordenadora Pedagógica: Élica Lopes

CÓDIGO:

240111033658

JÓSIS ALVES

Coordenador-científico dos cursos preparatórios para TI do Gran Cursos Online. Analista judiciário - área Tecnologia da Informação no Supremo Tribunal Federal (STF). Professor no Centro Universitário ESTÁCIO. Graduado em Informática pela Universidade do Grande Rio (Unigranrio); pós-graduado em Gestão da Segurança da Informação e Comunicações pela Universidade de Brasília (UnB); mestrando em Computação Aplicada pela UnB, área de concentração Segurança Cibernética (PPEE-UnB). Vasta experiência na área de ciência da computação, sistemas operacionais, engenharia e infraestrutura de redes com ênfase em Segurança da Informação. Além de fazer parte do rol de instrutores internos do Supremo Tribunal Federal.

GRAN CONCURSOS

SUMÁRIO

Apresentação 4
Apresentação e Propriedades Fundamentais 5
Questões de Concurso 7
Gabarito 9
Gabarito Comentado 10

APRESENTAÇÃO

Escrever um livro é algo desafiador. Porém, escrever para o público concurseiro torna a tarefa ainda mais árdua.

Afinal, há candidatos com diferentes níveis de conhecimento, estudando para seleções de áreas variadas.

No entanto, existe algo em comum entre aqueles que se preparam para um concurso público: **todos querem a aprovação** o mais rápido possível e **não têm tempo a perder**!

Foi pensando nisso que esta obra nasceu.

Você tem em suas mãos **um material sintético**!

Isso porque ele não é extenso, para não desperdiçar o seu tempo, que é escasso. De igual modo, não foge da batalha, trazendo tudo o que é preciso para fazer uma boa prova e garantir a aprovação que tanto busca!

Também identificará alguns sinais visuais, para facilitar a assimilação do conteúdo. Por exemplo, afirmações importantes aparecerão grifadas em azul. Já exceções, restrições ou proibições surgirão em vermelho. Há ainda destaques em **marca-texto**. Além disso, abusei de quadros esquemáticos para organizar melhor os conteúdos.

Tudo foi feito com muita objetividade, por alguém que foi concurseiro durante muito tempo.

Para você me conhecer melhor, comecei a estudar para concursos ainda na adolescência, e sempre senti falta de ler um material que fosse direto ao ponto, que me ensinasse de um jeito mais fácil, mais didático.

Enfrentei concursos de nível médio e superior. Fiz desde provas simples, como recenseador do IBGE, até as mais desafiadoras, sendo aprovado para defensor público, promotor de justiça e juiz de direito.

Usei toda essa experiência de 16 anos como concurseiro e de outros tantos ensinando centenas de milhares de alunos de todo o país para entregar um material que possa efetivamente te atender.

A Coleção PDF Sintético era o material que faltava para a sua aprovação!

Aragonê Fernandes

APRESENTAÇÃO DO PROFESSOR

Professor Jósis Alves é coordenador e professor dos cursos preparatórios para Tecnologia da Informação do GRAN, coordenador e professor da pós-graduação em Segurança da Informação da Gran Faculdade. Atualmente ocupa o cargo de Analista de Tecnologia da Informação (TI) e instrutor interno no Supremo Tribunal Federal (STF).

É graduado em Licenciatura em Informática, pós-graduado em Gestão da Segurança da Informação e Comunicações pela Universidade de Brasília (UnB). E atuou como docente em Instituição de Ensino Superior por vários anos.

APRESENTAÇÃO E PROPRIEDADES FUNDAMENTAIS

A segurança da informação é um aspecto crítico no mundo digital de hoje, onde dados e informações são ativos valiosos para qualquer organização. Com a crescente dependência de sistemas de informação para operações diárias e a proliferação de ameaças cibernéticas, a necessidade de proteger esses dados tornou-se mais importante do que nunca. A segurança da informação abrange diversas práticas e princípios destinados a proteger dados de acessos não autorizados, alterações, destruição ou divulgação. Essa proteção é vital não apenas para manter a confidencialidade e integridade da informação, mas também para garantir a disponibilidade, autenticidade, não-repúdio e confiabilidade. Estas propriedades formam a base para um ambiente de TI seguro e confiável, essencial para a preservação da privacidade, confiança e eficiência operacional em organizações de todos os tipos e tamanhos.

O tópico importante e basilar são as propriedades fundamentais da segurança da informação, essenciais para a proteção de dados em organizações. Estas propriedades são:

- **Confidencialidade**: Refere-se à **proteção contra a divulgação não autorizada de informações**. Exemplos incluem hospitais implementando controles de acesso e criptografia para proteger registros médicos e empresas financeiras utilizando criptografia SSL para proteger transações online.
- **Integridade**: Garante que **as informações não sejam alteradas ou destruídas de forma não autorizada**. Por exemplo, bancos usam sistemas de detecção de intrusões e verificações de hash para proteger transações financeiras, enquanto empresas de e-commerce empregam certificados digitais para assegurar a integridade das transações online.
- **Disponibilidade**: Assegura que **informações e recursos estejam acessíveis quando necessário**. Isso inclui empresas de TI investindo em redundâncias de servidores e conexões de internet, e provedores de serviços em nuvem implementando planos de recuperação de desastres.
- **Autenticidade**: Verifica a **origem e a autenticidade da informação**. Exemplos incluem o uso de certificados de autenticação para garantir a genuinidade de softwares e certificados SSL para validar a autenticidade de sites em transações online.
- **Não-repúdio (Irretratabilidade)**: **Impede que uma parte negue a autoria ou recebimento de uma mensagem ou transação**, comum em ambientes legais e comerciais. Isso pode ser assegurado por meio de assinaturas digitais e registros de auditoria.

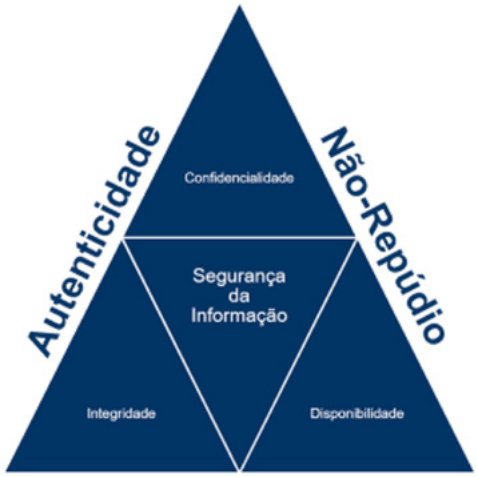


Figura 01: Propriedades da segurança da informação

- **Confiabilidade**: Garante que **sistemas ou informações funcionem de maneira precisa e consistente**. Exemplos incluem companhias aéreas com sistemas de reserva robustos e plataformas de e-commerce que implementam protocolos de entrega de mensagens confiáveis.

QUESTÕES DE CONCURSO

001. (IADES/CRF-TO/ANALISTA DE TI/2019) Um programa de segurança deve seguir os três princípios de segurança conhecidos como CIA. Quais são esses princípios?
a) Confidencialidade, interação e artifícios.
b) Confidencialidade, integridade e disponibilidade.
c) Montagem, infalibilidade e segurança.
d) Contenda, inatividade e arguição.
e) Concretude, inerência e disponibilidade.

002. (CESPE/CGM JOÃO PESSOA-PB/AUDITOR MUNICIPAL DE CONTROLE INTERNO – DESENVOLVIMENTO DE SISTEMAS/2018) Acerca de integridade, disponibilidade e confidencialidade em segurança da informação, julgue o item a seguir.
A disponibilidade pressupõe que uma informação deva estar disponível a qualquer pessoa de direito, sempre que necessário.

003. (CEBRASPE/BANESE/TÉCNICO BANCÁRIO I/2021) Confidencialidade, integridade e disponibilidade são princípios básicos de segurança da informação.

004. (FGV/SEFAZ-AM/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO DA FAZENDA ESTADUAL/2022) A administração de dados deve observar princípios básicos que são largamente adotados pela comunidade segurança da informação. Além da Confidencialidade, Integridade, Disponibilidade e Autenticidade, o princípio da Irretratabilidade completa a lista. Assinale o significado do princípio da Irretratabilidade.
a) Garantia de que os usuários que originam as informações são conhecidos e autorizados, de modo que não possam se passar por terceiros.
b) Impossibilidade de negação de que uma pessoa tenha sido autora de uma determinada informação.
c) Obrigatoriedade dos agentes pelo zelo com todas as informações coletadas.
d) Preservação fidedigna das informações.
e) Restrição de acesso às informações apenas aos autorizados.

005. (FGV/TJ-DFT/ANALISTA JUDICIÁRIO – SUPORTE EM TECNOLOGIA DA INFORMAÇÃO/2022) Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.

Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:
a) confidencialidade;
b) autenticidade;
c) integridade;
d) disponibilidade;
e) irretratabilidade.

006. (FGV/TCE-TO/ANALISTA TÉCNICO – TECNOLOGIA DA INFORMAÇÃO/2022) O auditor José recebeu o arquivo Anexo J em formato digital. Antes de proceder com a abertura do Anexo J, José determinou a fidedignidade do referido arquivo, avaliando a conformidade dos dados do Anexo J por ele recebido com os dados do Anexo J transmitido pelo emissor. Essa avaliação feita por José em Anexo J está diretamente relacionada com o seguinte princípio da segurança de informações:
a) integridade;
b) confidencialidade;
c) autenticidade;
d) disponibilidade;
e) qualidade.

007. (FGV/IMBEL/ANALISTA ESPECIALIZADO – ANALISTA DE SISTEMAS/2021) Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção.
Assinale o atributo que não é parte desse grupo.
a) Autenticidade.
b) Confidencialidade.
c) Disponibilidade.
d) Flexibilidade.
e) Integridade.

GABARITO

1. b
2. C
3. C
4. b
5. e
6. a
7. d

GABARITO COMENTADO

001. (IADES/CRF-TO/ANALISTA DE TI/2019) Um programa de segurança deve seguir os três princípios de segurança conhecidos como CIA. Quais são esses princípios?
a) Confidencialidade, interação e artifícios.
b) Confidencialidade, integridade e disponibilidade.
c) Montagem, infalibilidade e segurança.
d) Contenda, inatividade e arguição.
e) Concretude, inerência e disponibilidade.

A questão refere-se aos três princípios fundamentais da segurança da informação, conhecidos pela sigla CIA, que se refere a:

- Confidencialidade: Garantir que a informação seja acessível apenas por indivíduos autorizados, protegendo-a contra acesso não autorizado.
- Integridade: Assegurar que a informação seja mantida e transferida de maneira precisa e completa, sem ser alterada de forma maliciosa ou acidental.
- Disponibilidade: Garantir que a informação e os recursos relacionados estejam disponíveis quando necessário, especialmente durante situações críticas.

O gabarito corretamente identifica a opção B (Confidencialidade, Integridade e Disponibilidade) como os três princípios de segurança conhecidos como CIA. Esses princípios são a base para qualquer programa ou política de segurança da informação, e são essenciais para proteger os ativos de informação de uma organização contra ameaças e garantir a continuidade dos negócios.
Letra b.

---

002. (CESPE/CGM JOÃO PESSOA-PB/AUDITOR MUNICIPAL DE CONTROLE INTERNO – DESENVOLVIMENTO DE SISTEMAS/2018) Acerca de integridade, disponibilidade e confidencialidade em segurança da informação, julgue o item a seguir.
A disponibilidade pressupõe que uma informação deva estar disponível a qualquer pessoa de direito, sempre que necessário.

A disponibilidade é um dos três pilares fundamentais da segurança da informação, juntamente com a confidencialidade e a integridade, conforme representado pela Tríade CIA (Confidencialidade, Integridade e Disponibilidade).
A disponibilidade refere-se à garantia de que os dados e os recursos de informação estejam acessíveis às partes autorizadas sempre que necessário. Esse princípio é crucial para

garantir que os processos de negócios possam operar de forma eficiente e que as partes interessadas possam acessar as informações de que precisam para realizar suas funções de maneira eficaz.

No contexto da questão, a frase "qualquer pessoa de direito" implica em indivíduos ou sistemas que têm permissões adequadas para acessar a informação. Portanto, o princípio de disponibilidade não sugere que as informações devem estar disponíveis para todos indiscriminadamente, mas sim para aqueles que têm o direito ou a autorização para acessá-las. Isso está alinhado com as práticas recomendadas de segurança da informação que equilibram a necessidade de acesso à informação com a necessidade de proteger essa informação de acessos não autorizados.

Certo.

---

003. (CEBRASPE/BANESE/TÉCNICO BANCÁRIO I/2021) Confidencialidade, integridade e disponibilidade são princípios básicos de segurança da informação.

- Confidencialidade, integridade e disponibilidade, frequentemente referidos como o "Triângulo CIA" ou "Tríade CIA", são os três pilares fundamentais da segurança da informação. Esses princípios formam a base sobre a qual são construídas as políticas e medidas de segurança para proteger os dados digitais e os sistemas de informação. Vamos discutir cada um desses princípios em detalhe:
- Confidencialidade: Este princípio se refere à proteção de informações contra acesso não autorizado. Informações confidenciais, sejam elas pessoais, comerciais ou governamentais, devem ser acessíveis apenas por pessoas autorizadas. A violação da confidencialidade pode ocorrer por vários meios, como ataques cibernéticos, espionagem, vazamentos de dados, entre outros. Métodos para assegurar a confidencialidade incluem criptografia, autenticação forte, controle de acesso etc.
- Integridade: Integridade envolve a manutenção da precisão e consistência dos dados durante todo o seu ciclo de vida, garantindo que a informação não seja alterada de maneira não detectável por uma fonte não autorizada. Isto é crucial para decisões comerciais, processos legais, e saúde e segurança pessoal, entre outros campos. Medidas para proteger a integridade incluem controles de acesso, processos de mudança controlada, e sistemas de verificação, como somas de verificação e assinaturas digitais.
- Disponibilidade: Este princípio assegura que a informação esteja acessível e utilizável sob demanda por uma entidade autorizada. Isso significa que os sistemas que armazenam, processam e transmitem informações devem estar funcionando corretamente e sem interrupção. Ataques que podem afetar a disponibilidade incluem ataques de negação

de serviço (DoS) e danos físicos à infraestrutura de hardware. A disponibilidade pode ser mantida através de medidas como redundância de hardware, balanceamento de carga, sistemas de backup, recuperação de desastres e manutenção contínua.

Certo.

---

004. (FGV/SEFAZ-AM/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO DA FAZENDA ESTADUAL/2022) A administração de dados deve observar princípios básicos que são largamente adotados pela comunidade segurança da informação. Além da Confidencialidade, Integridade, Disponibilidade e Autenticidade, o princípio da Irretratabilidade completa a lista. Assinale o significado do princípio da Irretratabilidade.

a) Garantia de que os usuários que originam as informações são conhecidos e autorizados, de modo que não possam se passar por terceiros.

b) Impossibilidade de negação de que uma pessoa tenha sido autora de uma determinada informação.

c) Obrigatoriedade dos agentes pelo zelo com todas as informações coletadas.

d) Preservação fidedigna das informações.

e) Restrição de acesso às informações apenas aos autorizados.

Irretratabilidade (também conhecido como não repúdio) na segurança da informação. Vamos analisar o conceito e o motivo pelo qual essa é a resposta correta:

A Irretratabilidade ou não repúdio refere-se à capacidade de provar, de maneira irrefutável, que uma determinada ação ou evento ocorreu. Por exemplo, que uma mensagem foi enviada por uma pessoa específica, que alguém aprovou uma transação específica, ou que um acesso a um determinado sistema foi feito por um indivíduo em particular. Esse princípio é crucial em ambientes onde a negação de atividades realizadas pode ter consequências legais ou financeiras.

O não repúdio é frequentemente garantido através do uso de métodos de segurança eletrônica, como assinaturas digitais e certificados, que fornecem uma prova criptográfica de que uma determinada ação foi realizada por um indivíduo ou entidade identificável. Em termos simples, assegura que um autor de uma ação não possa negar a autoria de tal ação ou transação.

Letra b.

---

005. (FGV/TJ-DFT/ANALISTA JUDICIÁRIO – SUPORTE EM TECNOLOGIA DA INFORMAÇÃO/2022) Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma

revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.
Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:
a) confidencialidade;
b) autenticidade;
c) integridade;
d) disponibilidade;
e) irretratabilidade.

O cenário descrito na questão é um exemplo clássico de onde o princípio da irretratabilidade ou não repúdio é fundamental.
A irretratabilidade, no contexto da segurança da informação, é a garantia de que uma parte de uma transação não pode negar ter recebido uma transação nem que a outra parte não pode negar ter enviado uma transação. É usado em áreas onde é necessário um forte entendimento e prova de que uma determinada ação foi realizada por uma entidade específica, e essa ação não pode ser negada posteriormente.
No caso de Lucas, ele tentou negar a autoria das operações de trading que resultaram em prejuízo. No entanto, através do uso de registros de auditoria robustos e mecanismos de garantia de identidade (como logs detalhados, rastreamento de IP, talvez autenticação de dois fatores, assinaturas digitais, entre outros), a corretora foi capaz de provar, de maneira irrefutável, que Lucas realizou as operações em questão. Essa capacidade de provar que uma ação foi realizada por uma entidade específica, mesmo quando ela tenta negar tal fato, é o cerne do princípio da irretratabilidade.
Letra e.

---

006. (FGV/TCE-TO/ANALISTA TÉCNICO – TECNOLOGIA DA INFORMAÇÃO/2022) O auditor José recebeu o arquivo Anexo J em formato digital. Antes de proceder com a abertura do Anexo J, José determinou a fidedignidade do referido arquivo, avaliando a conformidade dos dados do Anexo J por ele recebido com os dados do Anexo J transmitido pelo emissor. Essa avaliação feita por José em Anexo J está diretamente relacionada com o seguinte princípio da segurança de informações:
a) integridade;
b) confidencialidade;
c) autenticidade;
d) disponibilidade;
e) qualidade.

A integridade dos dados é um dos princípios centrais da segurança da informação e se refere à exatidão, consistência e confiabilidade dos dados durante seu ciclo de vida. Isso significa que os dados não foram alterados de forma não autorizada desde que foram criados, transmitidos ou armazenados.

No contexto da situação apresentada, o auditor José está verificando se o arquivo Anexo J que ele recebeu é exatamente o mesmo que foi enviado pelo emissor, sem alterações ou corrupções durante o processo de transmissão. Ele quer ter certeza de que o arquivo é fidedigno, o que significa que ele não foi modificado de maneira inadequada, seja intencionalmente (por exemplo, por meio de um ataque cibernético) ou acidentalmente (por exemplo, devido a falhas no hardware ou software).

Letra a.

---

007. (FGV/IMBEL/ANALISTA ESPECIALIZADO – ANALISTA DE SISTEMAS/2021) Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção.

Assinale o atributo que não é parte desse grupo.

a) Autenticidade.

b) Confidencialidade.

c) Disponibilidade.

d) Flexibilidade.

e) Integridade.

A segurança da informação é fundamentada em vários princípios básicos que ajudam a orientar as políticas, os controles e os procedimentos que protegem os dados e os sistemas de informação. Os atributos mais comumente reconhecidos nesse contexto são:

- Autenticidade: Este atributo assegura que as informações são originárias da fonte anunciada e que não houve falsificação. É fundamental para validar a identidade de usuários, sistemas ou entidades e garantir que uma comunicação, transação ou qualquer tipo de intercâmbio de dados é legítimo.
- Confidencialidade: Refere-se à proteção de informações para que não sejam divulgadas ou acessadas por entidades não autorizadas. A confidencialidade é crucial para manter segredos comerciais, proteger informações pessoais sensíveis e manter a segurança nacional, entre outros.
- Disponibilidade: Este princípio assegura que os dados e os sistemas estão disponíveis para uso quando necessário. A disponibilidade é crucial para manter as operações

do dia a dia de organizações e garantir que usuários legítimos possam acessar as informações quando necessário.

- Integridade: A integridade dos dados se refere à garantia de que as informações são mantidas em um estado correto e não são alteradas de forma inapropriada, seja acidentalmente ou maliciosamente. A integridade é vital para a tomada de decisões precisas, a operação de sistemas e a manutenção da confiança nas atividades comerciais e pessoais.

Letra d.

Abra

caminhos

crie

futuros

gran.com.br