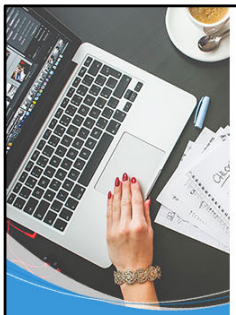
Fabio Sobiecki

PECC - Introdução



Introdução

Entendendo a certificação

Introdução à Certificação

Certified in Cybersecurity – a.k.a. Entry Level Certification

Não precisa ter experiência prévia

Preparar novos profissionais para a área de segurança

Validar os conhecimentos de pessoas que ainda não tem a devida experiência prática

Público Alvo

- Profissionais de TI
- Pessoas procurando transição de carreira para segurança
- Estudantes de Graduação ou recém-formados
- Pessoa que concluiu o ensino-médio

Tempo de exame e Idioma

- 2 horas
- Apresentar-se no centro de exames no mínimo 30 minutos antes
- Por enquanto, o exame está disponível apenas em Inglês
- Não é permitido dicionário

Número de questões

- 100 perguntas serão apresentadas
- 25% usadas para pesquisa
- Ao clicar no botão de próximo, não é possível voltar a pergunta anterior
- Múltipla escolha com 4 opções
  - 2 opções são incorretas
  - 2 opções são similares
  - Você deve escolher a mais correta
- 70% de acerto para passar

Manutenção da Certificação

- São necessários 45 CPEs
- Recomenda-se o mínimo de 15 CPEs por ano
- Taxa de 50 Dólares anuais, a partir do 1º aniversário

Processo de inscrição

1o. Inscrever-se na (ISC)2
https://my.isc2.org/s/login/SelfRegister

2o. Inscrever-se no exame
https://www.isc2.org/landing/CC-bundles

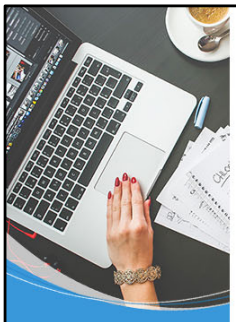
3o. Obter o exam outline
https://www.isc2.org/Certifications/CC/Certification-Exam-Outline

Ementa
Exam outline

- Conteúdo da prova
- Percentuais de cada assunto
- Detalhamento dos assuntos
- Áreas de conhecimento
  - Security Principles
  - Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
  - Access Controls Concepts
  - Network Security
  - Security Operations

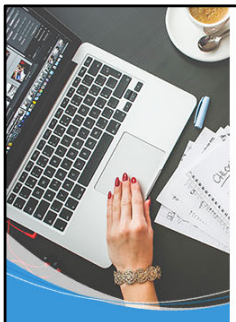
Exercício

- Inscreva-se para o Exame
- Baixe o Exam Outline



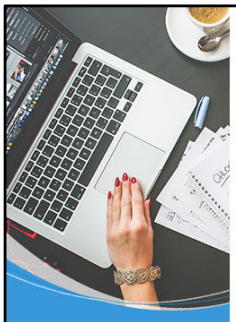
Princípios de Segurança

Entendendo os conceitos de segurança da garantia da informação

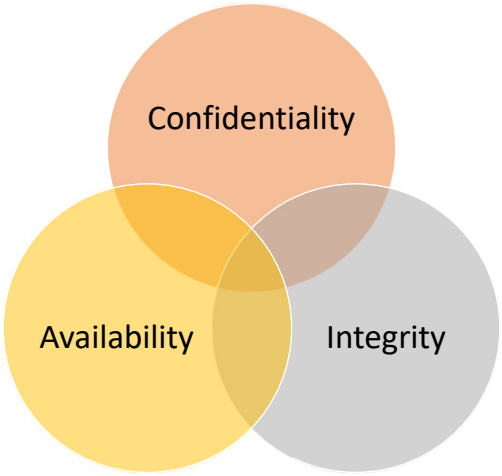


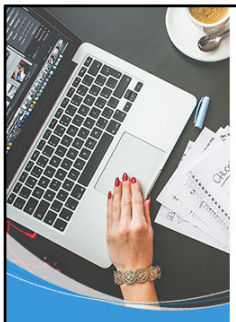
Visão Geral

Neste primeiro tópico vamos cobrir os princípios de segurança e a tríade CID. Depois vamos abordar o processo de gerenciamento de riscos. Em seguida vamos abordar os controles de segurança que farão a garantia dos pilares CID. Vamos abordar o controle organizacional de segurança e por fim abordar o código de ética da $(ISC)^2$.

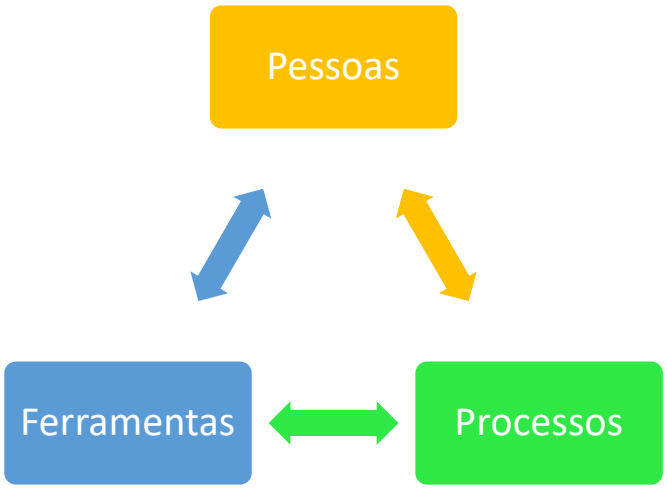


A Tríade CID





Segurança é feita de



Confidencialidade
confidentiality

- Ato de se manter o segredo de uma informação ou um ativo. A confidencialidade vai se basear na correta identificação de um ativo confidencial, a correta definição das pessoas que podem acessar aquele ativo e por fim, a correta garantia de proteção do ativo.

- Exemplo de ativos confidenciais:
  - Gabarito do Enem
  - Resultados de exames médicos
  - Transferências de dinheiro
  - Segredos industriais
  - Planos de marketing

Tipos de informação confidencial

- *Personally Identifiable Information (PII)* É um termo relacionado a confidencialidade, são informações de pessoas que podem fazer a identificação de um indivíduo.
- *Protected Health Information (PHI)* são informações de saúde de uma pessoa, que possui proteção específica *HIPAA - Health Insurance Portability and Accountability Act*
- *Classified* ou *Sensitive Information* – são informações que passaram por processo de

Confidencialidade
confidentiality

- Identificando Riscos e Ameaças
  - Vazamento da informação
  - Cópia ilegal
  - Venda da informação
  - Exposição vexatória

Confidencialidade
confidentiality

- Trabalhando a confidencialidade
  - Classificação de Informação (Pro)
  - Criptografia (Fer)
  - Controle de Acesso (Fer/Pro)
  - Dupla Diligência (Pro)
  - Treinamento de Pessoas (Pes)

Integridade
integrity

- É a garantia de que uma informação não foi substituída, removida parcialmente ou destruída. Se aplica na geração, processamento, armazenamento e em trânsito.

- Exemplos de necessidade de integridade em ativos:
  - Respostas do gabarito do enem;
  - Lista de devedores;
  - Voto eletrônico;
  - Notas de um aluno;
  - Saldo em conta;
  - Sentença do Juíz.

Integridade
integrity

- Identificando Riscos e Ameaças:
  - Alteração de dados;
  - Destruição de dados;
  - Ransomware;
  - Malwares;
  - Redes com problemas;
  - Falhas em dispositivos de armazenamento;
  - Crackers;
  - Má intenção do usuário.

Integridade
integrity

- Trabalhando a integridade:
  - Hash;
  - Cópia de segurança (Backup);
  - Clusters;
  - Réplicas;
  - Integridade Referencial;
  - CRC cyclic redundancy check;
  - Raid e bit de paridade.

Disponibilidade
availability

- Garantia de acesso à informação, no momento em que o usuário ou negócio necessitam da informação. Garantia da resiliência do Sistema que fornece acesso aos dados.
- Nem tudo precisa de alta disponibilidade, você deve identificar o que é crítico para a empresa.

- Exemplos de disponibilidade:
  - Sistemas com redundância;
  - Content Distribution Network CDN (akamai, cloudflare, cloudfront)
  - Arquitetura Distribuída

Disponibilidade
availability

- Identificando Riscos e Ameaças:
  - Denial of Service (DoS) ou Distributed Denial of Service (DDoS);
  - Ataques à infraestrutura
  - Interrupção devido à falhas (clima, política, criminalidade, ativismo, geológica, acidentes humanos)
  - Interrupção de serviço (Internet, Energia)
  - Erro humano

Disponibilidade
availability

- Trabalhando a Disponibilidade:
  - Arquitetura de alta disponibilidade;
  - Recursos redundantes;
  - Recursos de auto-recuperação;
  - Processos de checagem dupla.

Autenticação
authentication

- Processo de identificação de uma entidade para um Sistema computacional.
- Validar que a entidade em questão tem os direitos de acesso ao ativo.

- Métodos de autenticação:
  - O que você sabe: senha, pin, perguntas secretas
  - O que você tem: cartao, chaveiro, token, gerador otp
  - O que você é: face, digital, voz, retina, vasos sanguíneos
  - Como você faz: digitação, hábitos, movimentação mouse
  - Contexto que você está: rede, geolocalização, ip

Autenticação
authentication

- Single-fator, quando se usa um único método de autenticação
- Multi-fator, quando se usam vários métodos de autenticação
- Autenticação em duas etapas, quando se uma um método e em caso de sucesso, utiliza-se um segundo método

Não Repúdio

no-repudiation

- É um processo de garantia, para que uma pessoa não possa negar ter executado uma ação específica.

- Utilizamos para garantir, que um usuário que realiza uma aprovação ou acesso, não possa negar que o fez.

Não Repúdio
no-repudiation

- Trabalhando o não repúdio:
  - Certificado Digital;
  - Assinatura Digital;
  - Autenticação Biométrica.

Privacidade
privacy

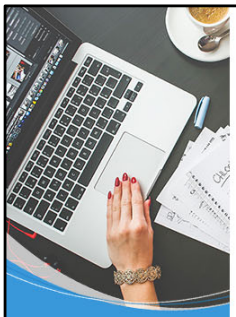
- É o direito de um indivíduo, de controlar a distribuição da informação de si mesmo.

- LGPD
- GDPR/EU
- Lei de privacidade da Califórnia
- PIPA Coréia do Sul

Exercício

Explique com suas palavras:

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticação
- Não Repúdio
- Privacidade



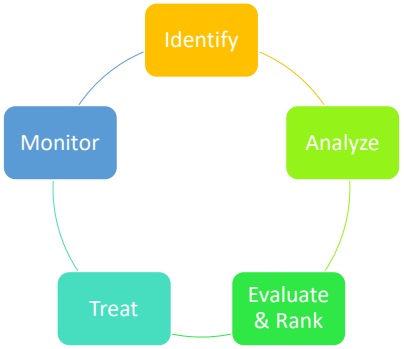
Princípios de Segurança

Entendendo o processo de gerenciamento de riscos

Gerenciamento de Risco

risk management

- Risco e segurança andam juntos o tempo todo.
- Avaliar e gerenciar os riscos da empresa é uma atividade recorrente.
- Existem diversos *frameworks* de gestão de risco, mas o mais aplicado é:



Gerenciamento de Risco

risk management

- Risco é definido como o quanto uma entidade (organização ou pessoa) é capaz de suportar a exposição à um evento ou circunstância.
- É normalmente medido com:
  - O impacto da situação adversa x a chance de ocorrer

- Ex. Dirigir um carro é se expor ao risco de se acidentar. E se isso ocorrer teremos danos materiais e/ou ferimentos aos passageiros x a chance de ocorrer.

Risco de Segurança da Informação
information security risk

- Risco de segurança da informação está relacionado ao impacto de uma adversidade caso ocorra um acesso não autorizado, uso não autorizado, vazamento de informação, interrupção de serviço, modificação ou destruição de dados.

- Alguns termos serão familiares durante a gestão de riscos:
  - *Asset* Ativo – algo a ser protegido. [documento, sistema, ambiente]
  - *Vulnerability* Vulnerabilidade – uma falha na proteção deste ativo
  - *Threat* Ameaça – Algo que utiliza uma vulnerabilidade para atingir um ativo

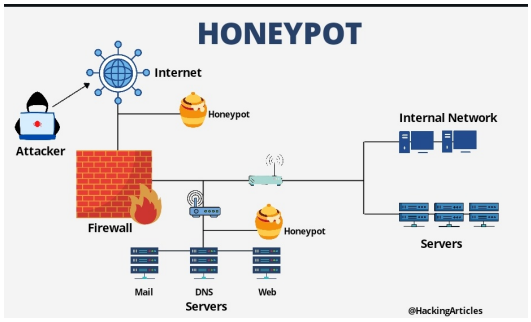
Vulnerabilidade
vulnerability

- Vulnerabilidade é uma fraqueza ou falha em um sistema ou seu componente, que pode levar à ocorrência de uma exploração.

Threat actor
atacante

Threat vector
Vetor de ataque ou
Método de ataque

Diminuir a percepção de vulnerabilidade



Ameaças
threats

- Uma ameaça é algo que utiliza uma vulnerabilidade para explorar com intuito maléfico.

- *Insiders* de uma empresa;
- Externos
- Empresas
- Entidades de Intel
- Tecnologia

Probabilidade e Impacto

likelihood and impact

- Ao analisar riscos, é obrigatório saber a probabilidade do risco se tornar real e em caso de se tornar real, qual o impacto?

- Isto te ajuda a priorizar o que pode ser mais prejudicial

Prioridades de Risco

risk priority

Likelihood	Impact: Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Tolerância à Riscos
risk tolerance

- Risco é relacionado com retorno financeiro.
- Algumas empresas tem um maior apetite à risco e outras um menor apetite à risco.
- Ao saber disso, o plano de gerenciamento de riscos pode mudar.

Identificação de Riscos
risk identification

- É um processo recorrente de avaliar e identificar possíveis pontos de problemas e então investigar se há riscos.

- Entrevistas
- Frameworks de Risco
- Comparação com outras empresas
- Histórico interno
- Oportunidades (mudanças, eventos)

Avaliação
Assessment

- Para cada problema investigado, identificar e quantificar o ativo, identificar e definir a probabilidade e o impacto de uma vulnerabilidade, identificar as possíveis ameaças, qualificar o risco por prioridade.
- Ex.: Implementar um novo Sistema de comércio eletrônico, em Outubro.
- Ex.: Upgrade do banco de dados de logística

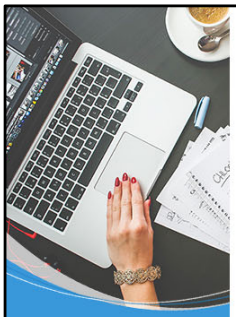
Tratamento de Riscos
Treatment

- Uma vez definido o risco e prioridade, sua empresa deve escolher entre:
  - Aceitar o risco: não fazer nada, apenas monitorar e reavaliar
  - Evitar o risco: fazer o possível para que diminuir ao máximo a probabilidade e/ou reduzir ao máximo o impacto
  - Mitigar o risco: fazer o possível para diminuir a probabilidade e o impacto
  - Transferir o risco: Assegurar um ativo para caso o risco ocorra, o impacto seja compartilhado

Monitoramento de Riscos

monitoring risks

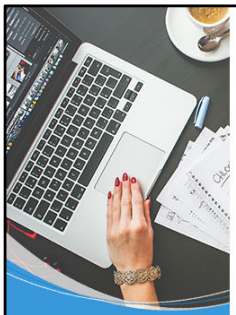
- Uma vez que o risco está consciente, devemos monitorar para saber se ele mudou ou foi eliminado.
- Isto é feito pelos ambientes que monitoram os status de saúde dos ativos de tecnologia
- Relatórios com resultados devem ser revisados pelos profissionais de segurança



Exercício

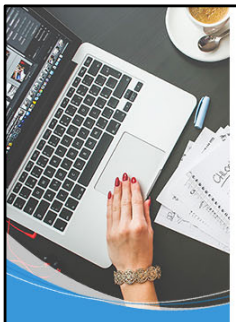
- Faça uma avaliação de riscos de uma faculdade:

1. Identificar riscos
2. Analizar riscos
3. Avaliar riscos
4. Tratar e Monitorar riscos



Princípios de Segurança

Entendendo os controles de segurança



Controles Técnicos
technical controls

- Quando se aplica um software ou mesmo um hardware, com a missão de coibir ou controlar ações dos usuários nos ativos.

- Ex. Autenticação, Autorização, Criptografia, Anti-virus, Firewalls.

Controles Administrativos
administrative controls

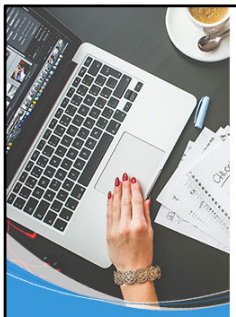
- São processos ou regras, aplicadas aos usuários para coibir ou controlar ações dos usuários nos ativos.

- Ex. Política de Senha, Exigência de autenticação Multi-fator.

Controles Físicos
physical controls

- Quando empregamos meios físicos e externos, para coibir ou controlar ações nos ativos.

- Ex.: Crachá por aproximação, catracas, portas com controle magnético, cofre de backup, cadeados de laptops, detectores de metais.



Princípios de Segurança

Entendendo o código de ética da (ISC)^2

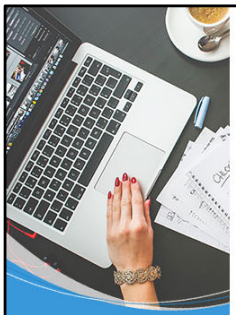
Código de conduta profissional
professional code of conduct

- Encontrar o Código no site
- Por que é importante?
- Infrações
- Denúncias

Exercícios

- Dê 5 exemplos de:
- Controles Físicos
- Controles Administrativos
- Controles Técnicos

Que não estejam entre os exemplos anteriores.



Princípios de Segurança

Entendendo o processo de governança

Governança de Segurança

security governance

- Qualquer empresa para se organizar precisa ter planejamento, tomada de decisões e uma visão de futuro. Isso que a Governança faz pela segurança, com base nos objetivos da empresa, a Governança organiza toda a área para cumprir as tarefas que levarão ao objetivo maior.

- Para isso, são definidas as políticas, procedimentos, padrões e identificadas as regulações que afetam a segurança da empresa.

Políticas
policies

- A política é um conjunto de regras, que define o que a empresa quer que o funcionário faça, naquelas situações específicas.
- O objetivo é que se tenha um comportamento padrão entre os funcionários, e que se faça o mais correto para preservar as informações.
- É escrita pela empresa, mas pode ser influenciada por fatores e frameworks externos.

Procedimentos
procedures

- São tutoriais com passo-a-passo que o funcionário deve executar, quando uma situação específica for necessária.

- Procedimento de backup;
- Procedimento de troca de discos;
- Procedimento de criação de um novo servidor.

- O objetivo é que não se esqueça de nenhum ponto importante e que seja um procedimento padronizado.

Padrões
standards

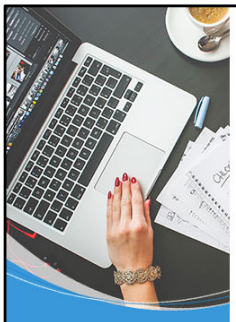
- Os padrões de segurança, são conjuntos de regras, políticas e procedimentos sugeridos para tipos de empresas similares.
- ISO 27001, NIST, ABNT, PCI/DSS
- O objetivo é enquadrar a empresa em um padrão conhecido para que os clientes possam confiar na segurança

Leis e Regulações
regulations and laws

- São todas as leis locais e internacionais, que podem afetar a segurança da informação direta ou indiretamente.
- Ex. LGPD, Marco Civil da Internet, GDPR, SOX, BACEN, HIPAA
- Algumas são leis, outras instruções normativas. Normalmente são mandatórias. A empresa que não cumpre está sugeita a sanções ou multas.

Exercícios

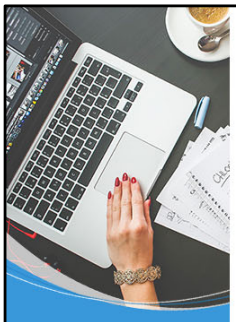
- Busque uma política de segurança e faça uma avaliação.
- Quais as regulações que estão sujeitas os planos de saúde?
- Busque uma cópia da ISO 27001



Pergunta 01

A chief information Security officer (CISO) at a large organization documented a policy that establishes the acceptable use of cloud environments for all staff. This is na example of:

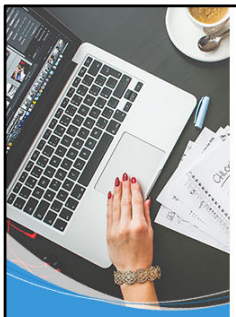
a) An adminsitrative control
b) A technical control
c) A physical control
d) A cloud control



Pergunta 01

A chief information Security officer (CISO) at a large organization documented a policy that establishes the acceptable use of cloud environments for all staff. This is na example of:

a) An adminsitrative control
b) A technical control
c) A physical control
d) A cloud control



Pergunta 02

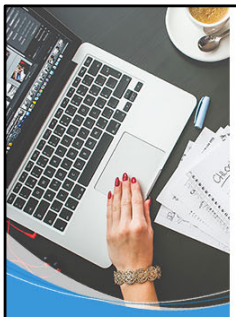
What is meant by nonrepudiation?

a) If a user does something, they can´t later claim that they didn´t do it.

b) Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.

c) It is part of the rules set by administrative controls.

d) It is a security feature that prevents session replay attacks.



Pergunta 02

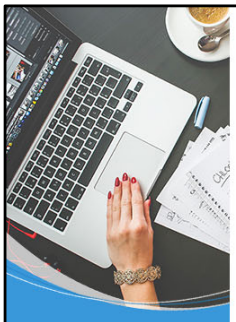
What is meant by nonrepudiation?

a) If a user does something, they can´t later claim that they didn´t do it.

b) Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.

c) It is part of the rules set by administrative controls.

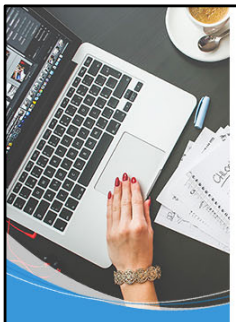
d) It is a security feature that prevents session replay attacks.



Pergunta 03

Which of the following is not one of the four typical ways of managing risk?

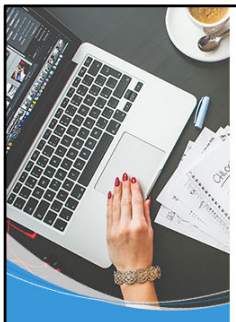
a) Avoid
b) Accept
c) Mitigate
d) Conflate



Pergunta 03

Which of the following is **not** one of the four typical ways of managing risk?

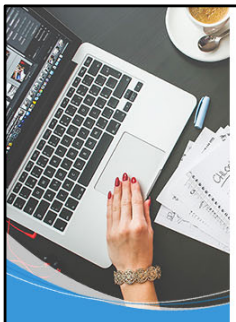
a) Avoid
b) Accept
c) Mitigate
d) Conflate



Pergunta 04

Siobhan is deciding wheter to make na online Purchase. The vendor wants Siobhan to create a new user account and requests Siobhan´s full name, home address, credit card number, phone number, email address, the ability to send marketing messages to Siobhan, and permission to share this data with other vendors. Siobhan decides that the item for sale is not Worth the value of Siobhan's personal information, and she decides not to make the Purchase. What kind of risk management approach did Siobhan take?

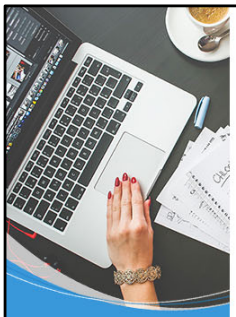
a) Avoidance
b) Acceptance
c) Mitigation
d) Transfer



Pergunta 04

Siobhan is deciding wheter to make na online Purchase. The vendor wants Siobhan to create a new user account and requests Siobhan´s full name, home address, credit card number, phone number, email address, the ability to send marketing messages to Siobhan, and permission to share this data with other vendors. Siobhan decides that the item for sale is not Worth the value of Siobhan's personal information, and she decides not to make the Purchase. What kind of risk management approach did Siobhan take?

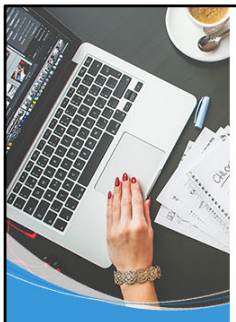
a) Avoidance
b) Acceptance
c) Mitigation
d) Transfer



Pergunta 05

Guillermo is the system administrator for a midsized retail organization. Guillermo has been tasked with writing a document that describes, step-by-step, how to securely install the operating system on a new laptop. This document is an example of:

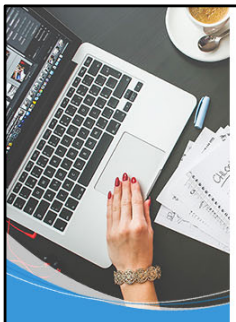
a) A policy
b) A standard
c) A procedure
d) A guideline



Pergunta 05

Guillermo is the system administrator for a midsized retail organization. Guillermo has been tasked with writing a document that describes, step-by-step, how to securely install the operating system on a new laptop. This document is an example of:

a) A policy
b) A standard
c) A procedure
d) A guideline



Pergunta 06

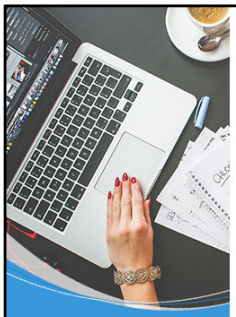
Lankesh is the Security administrator for a small food-distribution company. A new law is published by the country in which Lankesh's company operates. This law conflicts with the company's polices. Which Governance element should Lankesh's company follow?

a) The law

b) The policy

c) Any procedures the company has created for those activities affected by the law

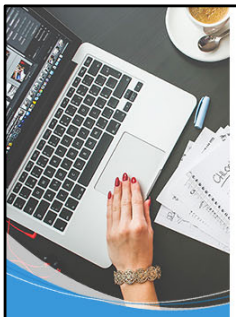
d) Lankesh should be allowed to use personal and professional judgment to make the determination of how to proceed.



Pergunta 06

Lankesh is the Security administrator for a small food-distribution company. A new law is published by the country in which Lankesh's company operates. This law conflicts with the company's polices. Which Governance element should Lankesh's company follow?

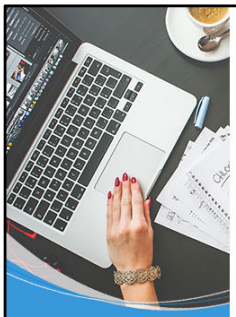
a) The law
b) The policy
c) Any procedures the company has created for those activities affected by the law
d) Lankesh should be allowed to use personal and professional judgment to make the determination of how to proceed.



Pergunta 07

Kristal is the Security administrator for a large online service provider. Kristal learns that the company is harvesting the personal data of its customers then sharing the data with local governments where the company operates without the knowledge of the users. This leads to these governments persecuting users for their political and philosophical beliefs. The published user agrement states that the company will not share personal user data with any entitites without the user's explicit permission. According to the ISC2 code of ethics, to whom does Kristal ultimately owe duty in this situation?

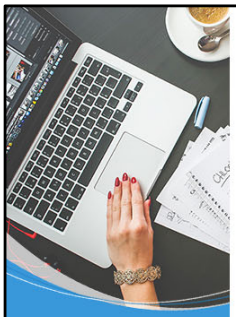
a) The governments of the countries where the company operates
b) The company for which Kristal works
c) The users
d) $(ISC)^2$



Pergunta 07

Kristal is the Security administrator for a large online service provider. Kristal learns that the company is harvesting the personal data of its customers then sharing the data with local governments where the company operates without the knowledge of the users. This leads to these governments persecuting users for their political and philosophical beliefs. The published user agrement states that the company will not share personal user data with any entitites without the user's explicit permission. According to the ISC2 code of ethics, to whom does Kristal ultimately owe duty in this situation?

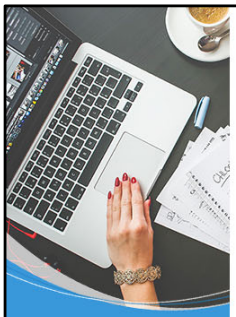
a) The governments of the countries where the company operates
b) The company for which Kristal works
c) The users
d) $(ISC)^2$



Pergunta 08

While taking the exam for this certification, you notice another candidate for the certification cheating. What should you do?

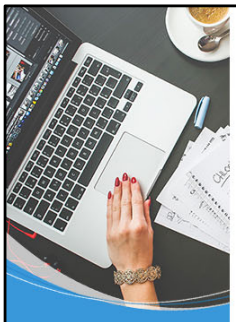
a) Nothing, as each person is responsible for their own actions
b) Yell at the other candidate for violating test security
c) Report the candidate to ISC2
d) Call local law enforcemnet



Pergunta 08

While taking the exam for this certification, you notice another candidate for the certification cheating. What should you do?

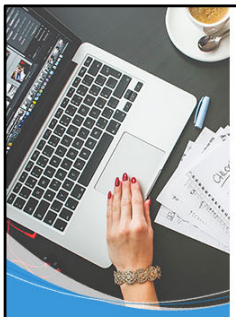
a) Nothing, as each person is responsible for their own actions
b) Yell at the other candidate for violating test security
c) Report the candidate to ISC2
d) Call local law enforcemnet



Pergunta 09

The concept of “secrecy” is most related to which foundational aspect of security?

a) Confidentiality
b) Integrity
c) Availability
d) Plausibility



Pergunta 09

The concept of “secrecy” is most related to which foundational aspect of security?

a) Confidentiality
b) Integrity
c) Availability
d) Plausibility