SEGURANÇA DA INFORMAÇÃO I

O tema de hoje, Segurança da Informação, merece destaque, pois tem mudado significativamente ao longo do tempo. A cobrança não é mais básica como há alguns anos, exigindo maior aprimoramento dos candidatos para evitar surpresas na prova.

Serão abordados diversos tópicos relacionados à segurança da informação, sem uma ordem específica. Esses tópicos podem coincidir com os do edital, mesmo que a nomenclatura varie. Por exemplo, alguns editais mencionam criptografia explicitamente, enquanto outros a incluem sob o título geral de segurança da informação. Todo o conteúdo discutido estará presente no edital ou poderá ser cobrado na prova. Portanto, é essencial que os candidatos se baseiem nesses pontos para uma preparação adequada.

TÓPICOS DA AULA

- Conceitos básicos e segurança da informação;
- Procedimentos de segurança;
- Noções de Segurança da Informação;
- Discrição e segurança de informações;
- Graus de sigilo;
- Atributos básicos;
- Ameaças e vulnerabilidade;
- Comportamento do agente Procedimentos de segurança;
- Noções de vírus e pragas virtuais;
- Aplicativos de segurança (antivírus, firewall, anti spyware, etc.).

Esta aula é inteiramente voltada para concursos, com o objetivo específico de preparar os candidatos, não para especialização ou aplicação profissional. Alguns termos usados podem não ser tão técnicos, mas são eficazes para responder questões de concursos. A explicação empírica ajuda na compreensão e marcação correta das respostas. Recomenda-se fazer anotações e resumos durante a aula para evitar a necessidade de rever o conteúdo. Caso surjam dúvidas não abordadas, estas devem ser enviadas para o fórum de dúvidas, onde serão esclarecidas.

5m

SEGURANÇA DA INFORMAÇÃO

- **Ativo:** Qualquer recurso, informação ou componente que tenha valor para uma organização, como dados, hardware, software ou propriedade intelectual.

É importante destacar que as pessoas também são consideradas ativos e devem ser protegidas. Isso se relaciona diretamente com o comportamento do agente, pois as pessoas desempenham um papel crucial na segurança da informação. Caso ocorra um descuido e informações fiquem acessíveis a indivíduos internos ou externos sem autorização, podem surgir ataques.

Os ataques podem ser internos, realizados por pessoas mal-intencionadas dentro da organização que acessam e compartilham informações indevidamente. Os ataques também podem ser externos, resultantes de um descuido. Por exemplo, um indivíduo com acesso a informações sigilosas que deixa esses dados expostos ao sair para tomar um café.

Assim, um ativo é tudo aquilo que deve ser protegido, não se limitando apenas aos dados, mas incluindo também as pessoas e seus comportamentos.

- **Vulnerabilidade:** Uma fraqueza ou falha em um sistema, processo ou procedimento que pode ser explorada por uma ameaça para causar danos ou comprometer a segurança.

Considere a vulnerabilidade ao término de um relacionamento: a pessoa se torna suscetível a um ataque de alguém mal-intencionado que deseja explorar essa fraqueza. Analogamente, uma vulnerabilidade em sistemas é uma falha de segurança que pode ser explorada por um atacante.

Quando um sistema está vulnerável, está suscetível a ataques, assim como uma pessoa emocionalmente frágil pode ser manipulada. Uma vulnerabilidade em sistemas pode ser uma falha ou brecha que um atacante pode explorar. Isso pode ser algo tão simples como uma porta que não tranca corretamente.

Muitos acreditam que segurança da informação se resume a antivírus e firewalls, mas também envolve a segurança física. Por exemplo, uma porta que não tranca corretamente em uma casa representa uma vulnerabilidade que um ladrão pode usar para invadir. Da mesma forma, em sistemas, vulnerabilidades podem ser encontradas em softwares, e atacantes estão constantemente buscando essas brechas para invadir sistemas.

Portanto, é crucial entender que segurança da informação abrange tanto aspectos físicos quanto digitais.

- **Ameaça:** Qualquer evento ou entidade que possui o potencial de explorar vulnerabilidades em um ativo e causar um incidente de segurança, como um ataque cibernético, desastre natural ou erro humano.

Fontes: https://www. nist. gov/ e https://www. iso. org/iso-iec-27001

A ameaça é qualquer evento ou entidade com o potencial de explorar vulnerabilidades em um ativo e causar um incidente de segurança, como um ataque cibernético, desastre natural ou erro humano. A ameaça pode ser bastante ampla, não se restringindo apenas a ataques humanos, mas abrangendo uma variedade de situações que podem comprometer a segurança. Por exemplo, uma pessoa emocionalmente vulnerável pode ser ameaçada por alguém que se aproveite dessa condição.

10m

SEGURANÇA DA INFORMAÇÃO

- **Risco:** A probabilidade de uma ameaça explorar vulnerabilidades em um ativo, resultando em um impacto negativo. O risco é geralmente avaliado como uma combinação da probabilidade da ameaça ocorrer e do impacto potencial.

Alguns termos importantes incluem risco, probabilidade e vulnerabilidade. O risco é a probabilidade de uma ameaça explorar uma vulnerabilidade em um ativo. Por exemplo, uma pessoa emocionalmente vulnerável após o término de um relacionamento corre maior risco de ser explorada.

A conscientização dos riscos pode reduzir a probabilidade de ocorrência de incidentes. Quando uma pessoa está ciente dos riscos e das suas vulnerabilidades, o risco é menor. No entanto, quando uma pessoa está completamente vulnerável, sem percepção dos riscos, a probabilidade de ser explorada é significativamente maior.

No contexto empresarial, a presença de múltiplas vulnerabilidades, sejam físicas ou lógicas, aumenta o risco. Um exemplo prático é a presença de pessoas não confiáveis dentro de uma organização. Já ocorreu em um órgão público em Brasília, onde terceirizados procurados pela justiça foram detectados, apesar das análises realizadas para a contratação. Esses indivíduos tinham acesso a áreas sensíveis, representando um risco significativo para a segurança da informação.

A questão do acesso não se limita ao grau hierárquico. O diretor de uma empresa pode não ter acesso irrestrito ao banco de dados, enquanto funcionários de níveis inferiores podem ter acesso devido à natureza técnica de suas funções. Isso se aplica também ao pessoal de limpeza, que frequentemente tem acesso a áreas altamente sigilosas. Esse acesso representa um risco considerável, semelhante ao risco presente em residências onde empregados domésticos podem ter acesso a informações e áreas sensíveis.

Portanto, é crucial reconhecer e mitigar esses riscos para garantir a segurança de informações e ativos tanto em ambientes profissionais quanto pessoais.

- **Prejuízo:** A perda financeira, danos à reputação, interrupção de serviços ou qualquer outro efeito negativo resultante da exploração de vulnerabilidades por uma ameaça.

No contexto descrito, ocorreu um incidente significativo, resultando em perda financeira, danos à reputação e interrupção dos serviços da empresa. Por exemplo, alguém desligou o banco de dados ou um servidor, causando paralisação das operações da empresa e afetando suas vendas e funcionamento regular. Tais efeitos negativos são consequências da exploração de vulnerabilidades por uma ameaça que acessou indevidamente as instalações.

É importante considerar como a segurança da informação pode ser aplicada no cotidiano, não se restringindo apenas a corporações ou ambientes de trabalho específicos. Mesmo para quem não vivencia diretamente essas situações, como estudantes ou pessoas em outras áreas, é relevante integrar conceitos de risco e vulnerabilidade na rotina diária e em relacionamentos pessoais. Isso permite uma compreensão mais prática e aplicável desses conceitos. Quando se compreende a lógica por trás desses princípios, como os impactos de incidentes de segurança, torna-se mais fácil reconhecer sua importância e aplicá-los em diferentes contextos.

15m

- **Impacto:** O efeito ou consequência que um incidente de segurança pode ter sobre um ativo ou uma organização. O impacto pode ser financeiro, operacional, legal, entre outros.

Fontes: https://www. nist. gov/ e https://www. iso. org/iso-iec-27001

Então, prejuízo refere-se ao que foi perdido, como por exemplo, uma perda financeira significativa devido à interrupção das vendas por um período curto, o que pode representar milhões em prejuízo. No entanto, o impacto não se limita apenas ao aspecto financeiro. Ele também envolve as consequências mais amplas de um incidente, como danos à reputação e à confiança dos clientes.

Por exemplo, em um órgão cujo foco principal é a segurança, a violação dessa segurança pode ter um impacto devastador na imagem da empresa. Mesmo que não haja um prejuízo financeiro imediato pelo acesso não autorizado ou furto de objetos, as repercussões podem ser severas. A percepção pública de uma empresa de segurança comprometida pode levar à perda de clientes e confiança no serviço oferecido.

Portanto, é essencial considerar não apenas os aspectos financeiros, mas também as implicações mais amplas de violações de segurança, ao fazer anotações sobre esses pontos durante o estudo.

DADOS

A proteção da informação é um tema amplamente discutido, mas é crucial entender o que se pretende proteger. O conceito de informação pode ser questionado: o que realmente define informações? Para compreendê-lo, é necessário começar pelos dados, que são informações brutas como números e letras.

Assim, antes de abordar estratégias de proteção, é fundamental definir claramente o que constitui informações e como os dados se relacionam com esse conceito.

b s h e 1 g 9 u 5 a 0 1 s 3 1 o 2 à 7 o 6 n c

Ao apresentar esse conteúdo, pode não ser imediatamente compreensível para o leitor, uma vez que consiste apenas em letras e números aleatórios que não são intuitivamente legíveis por seres humanos. Nesse contexto, esses elementos são denominados dados. A transformação ocorre quando esses dados são processados e adquirem significado. Organizando-os de maneira estruturada, é possível convertê-los em informações compreensíveis. No entanto, nem todos os conjuntos de dados podem ser organizados dessa forma para se tornarem informações úteis.

INFORMAÇÃO

O Bogo nasceu 12/05/1976 às 13h

Ao processar e analisar um conjunto de dados, obtém-se uma informação. Por exemplo, ao organizar letras e números de maneira coerente, como “às 13 horas”, gera-se uma informação compreensível. Assim, dados processados e compreensíveis são denominados informações.

O próximo passo é a utilização dessa informação. Utiliza-se como exemplo os mapas astrais: pode-se usar a data e o horário de nascimento para gerar um mapa astral. A partir da informação sobre a data e horário de nascimento, pode-se gerar um conhecimento específico.

Portanto, há uma progressão: dados brutos são processados e analisados, tornando-se informações; essas informações podem, mas não necessariamente, gerar conhecimento. No exemplo citado, conhecer a data e horário de nascimento de Bogo pode permitir a criação de um mapa astral, que poderia até servir como presente de aniversário.

É crucial lembrar que nem toda informação gerará conhecimento, assim como nem todos os dados se transformarão em informações significativas. Embora isso não seja frequentemente explorado em provas, é importante estar ciente dessa distinção.

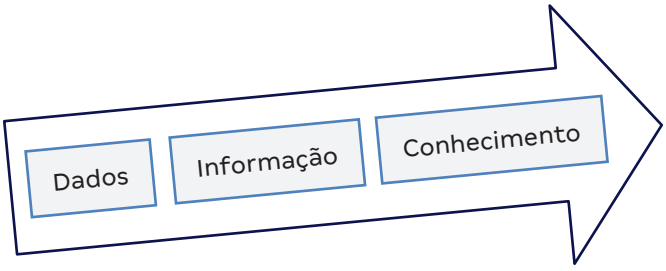
20m

CONHECIMENTO

Ao analisar e processar dados, obtém-se uma informação. Quando essa informação é analisada, pode-se extrair dela um conhecimento. O passo seguinte é a aplicação desse conhecimento, denominada sabedoria ou inteligência. Esse processo envolve utilizar o conhecimento de maneira prática e eficaz.

Por exemplo, ao estudar segurança da informação, inicialmente trabalha-se com dados brutos, como textos que podem parecer incompreensíveis. Ao processar esses dados, gera-se uma informação. Analisando essa informação, adquire-se conhecimento sobre o tema. A sabedoria, então, consiste em aplicar esse conhecimento, como em uma prova.

Muitas pessoas possuem o conhecimento, mas não conseguem aplicá-lo de forma inteligente. Saber responder sobre criptografia, por exemplo, requer não apenas a memorização de métodos, mas a capacidade de interpretar e aplicar essa informação corretamente em um contexto prático. Portanto, a sabedoria é o estágio final e mais importante, que envolve a aplicação eficaz do conhecimento adquirido.



O processo inicia-se com dados, que ao serem analisados e processados, transformam-se em informação. Esta informação, quando devidamente interpretada, gera conhecimento. O estágio final desse processo é a sabedoria ou inteligência, que se refere à aplicação prática desse conhecimento.

1. (2022/INSTITUTO AOCP/IFRO/ASSISTENTE EM ADMINISTRAÇÃO)
Preencha as lacunas e assinale a alternativa correta. Para alcançar grande compreensão acerca de algo, segundo as teorias que versam sobre os gestão da informação, ocorre, de maneira simplória, um processo que envolve _____, que são registros soltos e aleatórios de algo que, após serem estruturados e organizados, passam a ser definidos como _____ e então, quando processados, se transformam em _____.

a. informação / compreensão / comunicação
b. conhecimento / dados / informação
c. dados / comunicação / conhecimento
d. informação / dados / comunicação
e. dados / informação / conhecimento

Para alcançar uma compreensão aprofundada sobre um tema, segundo as teorias que tratam da gestão da informação, ocorre um processo que envolve registros soltos e aleatórios de algo. Isso remete a dados. Portanto, pode-se eliminar alternativas como informação e conhecimento, focando apenas nas que se referem a dados. Após serem estruturados e organizados, esses dados passam a ser definidos como informação.

GABARITO

1. e