SEGURANÇA DA INFORMAÇÃO II

DIRETO DO CONCURSO

2. (2023/IFMT /TÉCNICO DE LABORATÓRIO) As sentenças abaixo são inspiradas no texto de Ramos (2006) sobre Segurança da Informação:

I – Evento que tem potencial em si próprio para comprometer os objetivos da organização e pode trazer danos diretos aos ativos, ou prejuízos decorrentes de situações inesperadas.
II – Ausência de um mecanismo de proteção ou falhas em um mecanismo de proteção existentes.
III – Medida indicativa de probabilidade de uma ocorrência que possa comprometer os objetivos da organização, combinada com os impactos que ela trará.

Tais sentenças descrevem, respectivamente, as definições de:
a. Ameaça, Vulnerabilidade e Risco.
b. Vulnerabilidade, Ameaça e Impacto.
c. Ameaça, Risco e Prejuízo.
d. Impacto, Ameaça e Prejuízo.
e. Risco, Vulnerabilidade e Impacto.

3. (2023/OBJETIVA CONCURSOS/PREFEITURA DE PIRATININGA/ASSISTENTE SOCIAL) Sobre os conceitos de dados na tecnologia da informação, analisar os itens abaixo:

I – Os sistemas computacionais trabalham basicamente com dados e sua função é o processamento desses dados.
II – Pode-se entender o dado como um elemento da informação (um conjunto de letras ou dígitos) que, tomado isoladamente, não transmite nenhum conhecimento e não contém um significado intrínseco.
III – Dados são materiais brutos que precisam ser manipulados e colocados em um contexto compreensivo antes de se tornarem úteis.

Está(ão) CORRETO(S):
a. Somente o item I.
b. Somente o item II.
c. Somente os itens I e III.
d. Todos os itens.

5m

I – Em suma, o computador e os sistemas computacionais, de modo geral, têm como função processar dados.
II – Dado é um elemento da informação que, isoladamente, não é compreensível.
III – Os dados, por si só, não são úteis. Dados isolados não são compreensíveis e, portanto, não têm utilidade nesse caso.

SEGURANÇA DA INFORMAÇÃO

Na segurança da informação, não se deve focar apenas nos programas. O escopo de proteções inclui diversos aspectos que precisam ser considerados para uma compreensão completa do tema.

- **SEGURANÇA FÍSICA.**
- **SEGURANÇA LÓGICA.**

SEGURANÇA FÍSICA

Fonte: https://gestaodesegurancaprivada.com.br/seguranca-fisica-e-do-ambiente-definicao/

A segurança física envolve a proteção e o controle de acesso às instalações, bem como a proteção física dos materiais utilizados. Isso inclui elementos como portas e paredes. Houve uma questão em prova, em que foi mencionado que uma porta de vidro comum, a menos que especificado como vidro especial ou blindado, deveria ser considerada apenas uma porta de vidro comum. A questão perguntava se uma porta de vidro comum poderia proteger contra ações de vândalos. A interpretação correta é que uma pessoa comum

pode ser impedida por uma porta trancada, mas um vândalo, que busca causar danos, provavelmente quebraria a porta com um objeto. Se o vidro não for especial, como vidro blindado, a porta não oferecerá resistência suficiente contra ações agressivas.

10m

A interpretação de texto é essencial e deve ser feita com base nas informações fornecidas no texto, sem extrapolações injustificadas.

Às vezes, uma câmera pode ser considerada uma barreira física, pois o monitoramento influencia o comportamento de pessoas normais que sabem estar sendo filmadas. Conforme mencionado, para muitas pessoas, o fato de serem filmadas pode não interferir em suas ações. No entanto, para alguém com intenções erradas, a presença da câmera pode interromper suas ações. Esse indivíduo pode pensar: "Não vou fazer isso porque sei que estou sendo filmado e serei responsabilizado por tal ação".

Portanto, uma porta é utilizada para impedir que uma pessoa não autorizada entre no local e furte tanto dados quanto outros ativos.

Fonte: https://www.diegomacedo.com.br/introducao-a-seguranca-fisica

Essa pessoa pode estar transferindo dados, por exemplo, utilizando um pen drive ou HD externo, acessando informações de forma indevida ou até mesmo levando equipamentos. Todas essas ações podem causar prejuízos à empresa.

Então, existe aqui uma porta que serve para reforçar essa questão. Essa porta não será facilmente acessada, embora não se possa afirmar que seja impossível transpô-la. Atualmente, há crimes violentos ocorrendo em todo o Brasil, em que pessoas utilizam explosivos para entrar em locais e causar destruição. Portanto, não se trata de uma situação impossível. No entanto, ao considerar esta imagem isoladamente, é evidente que uma porta desse tipo não serve para nada se estiver aberta ou destrancada. Mais adiante, será abordada a correlação desses conceitos.

Há um livro escrito por Kevin Mitnick, um hacker americano, que introduziu o conceito de "engenharia social", um assunto que será explorado posteriormente. Mitnick destacou que a maior vulnerabilidade e risco à segurança são as pessoas. Quando se deseja obter informações de alguém, é fundamental perguntar diretamente. Alguém poderia argumentar: "Mas se alguém me perguntar a senha do meu email, eu não vou fornecê-la". Aí entra a engenharia social, que visa obter informações que levem à senha sem mencioná-la diretamente.

Portanto, as pessoas representam um grande risco para as empresas. De nada adianta ter uma porta de segurança se alguém tem a chave ou o código de acesso. Em muitos casos, essas informações podem ser obtidas por meio de engenharia social. Ao conversar com as pessoas, um invasor pode obter informações que facilitam a entrada, persuadindo a pessoa a acreditar que está obtendo um benefício. Um exemplo disso é ligar para os clientes, fingindo ser do provedor de internet, e sugerir melhorias na conexão para obter informações sensíveis, como senhas ou códigos de acesso. Assim, como Mitnick sempre enfatizou, as pessoas são um dos maiores riscos à segurança da informação.

As catracas também são exemplos de barreiras físicas. É claro que uma pessoa comum não ultrapassaria a catraca indevidamente. Nesse contexto, a utilização de uma porta devidamente trancada oferece a possibilidade de prevenir ambos os casos mencionados.

Aqui é apresentado um exemplo da sala conhecida como sala cofre. Essas salas possuem diversos níveis de proteção, sendo totalmente blindadas contra fogo e água, inclusive inundação. É importante observar que todas essas proteções têm limitações, como temperatura, quantidade e pressão da água, entre outros. No entanto, essas salas são extremamente seguras. Todavia, todas essas medidas de segurança se tornam inúteis se a porta for deixada aberta, possibilitando a entrada de indivíduos não autorizados, o que pode resultar em danos significativos para a empresa.

15m

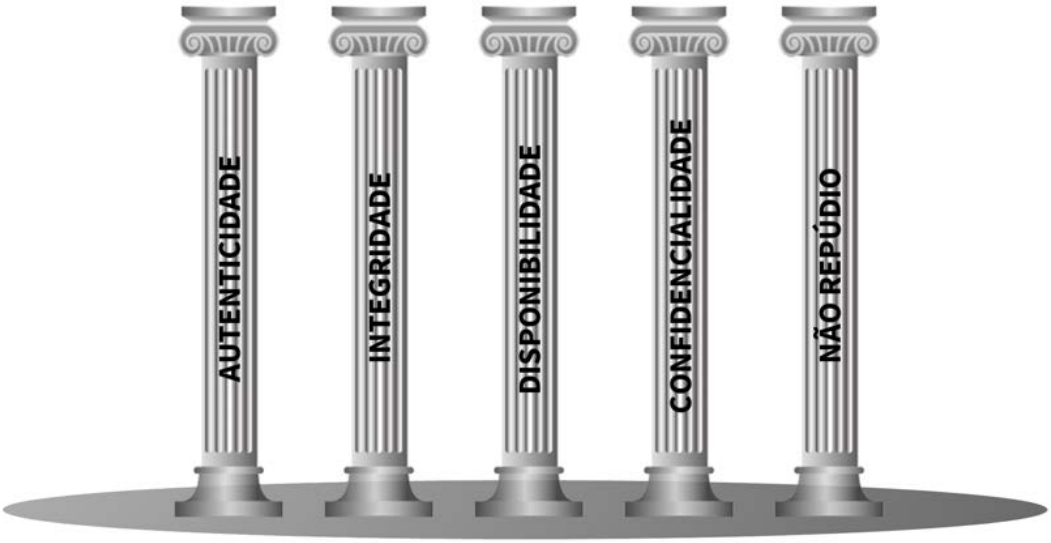
SEGURANÇA LÓGICA

É essencial ter em mente que a segurança da informação não se limita apenas a softwares. Inclui também a segurança física. Uma porta deixada aberta pode acarretar em grandes prejuízos, caso seja esquecida assim em um local indevido e acessada por pessoas não autorizadas. No entanto, com a aplicação adequada da segurança lógica, mesmo nessas situações, a pessoa pode não conseguir alcançar seu objetivo de acessar informações sensíveis. Por isso, a importância da integração entre segurança física e lógica, sendo ideal que a porta esteja sempre trancada e que medidas de segurança lógica estejam igualmente implementadas.

PILARES DA SEGURANÇA DA INFORMAÇÃO

O objetivo de um pilar é proporcionar sustentação, como se pode observar numa construção física. Analogamente, em um relacionamento, é fundamental haver confiança mútua. A desconfiança constante em relação a outra pessoa pode gerar desconforto e inquietação. Não se trata de investigar a pessoa, mas de estabelecer uma base sólida em que a confiança mútua é preservada. No entanto, uma quebra de confiança pode ocorrer se descobertas revelarem ações contrárias às expectativas.

De maneira análoga, na segurança da informação, a confiança desempenha um papel crucial. Se uma porta é deixada aberta, mesmo que medidas lógicas estejam em vigor para proteger os dados, o comprometimento da segurança já ocorreu. Portanto, é essencial avaliar o contexto completo para entender as consequências de uma falha de segurança, mesmo que inicialmente pareça protegida.



Os pilares da segurança da informação são a autenticidade, a integridade, a disponibilidade, a confidencialidade e o não repúdio.

AUTENTICIDADE

O que é ser autêntico? Ser autêntico significa comprovar sua identidade de forma inequívoca. Não basta apenas afirmar quem se é; é necessário fornecer uma garantia concreta. Em se tratando de uma assinatura digital, por exemplo, utilizando um certificado digital emitido por uma empresa, há uma validação externa que confirma a identidade de uma pessoa em transações online. Este processo oferece uma garantia razoável de autenticidade, embora não seja completamente infalível. Isso ressalta um princípio fundamental na segurança da informação: não existe garantia total em qualquer contexto.

20m

Na segurança da informação, não se pode afirmar que existe proteção absoluta. Imagine construir uma sala-cofre com uma porta blindada, reforçada com medidas adicionais. Ainda assim, é importante lembrar que alguém possui o código de acesso para essa sala. Independentemente de ser uma ou mais pessoas, em algum momento essa porta pode ficar desprotegida, invalidando a ideia de proteção total.

Considera-se também o investimento em softwares de alta segurança, destacando a necessidade de interpretação integrada. Quanto maior o nível de segurança implementado, geralmente, maior a complexidade e o tempo necessários para acessar determinados recursos. Por exemplo, ao acessar uma sala, pode ser exigido um processo extenso de autenticação: verificação da íris, biometria digital, senha, entre outros procedimentos, impactando diretamente na velocidade de acesso.

É crucial encontrar um equilíbrio entre a segurança aplicada e a eficiência operacional. Em algumas situações, mais segurança pode significar maior lentidão ou dificuldade de acesso, enquanto em outras, reduzir as medidas de segurança pode proporcionar maior fluidez. Uma analogia pertinente pode ser feita com o trânsito: em caso de acidente sem vítimas, a remoção rápida do veículo para restaurar a fluidez é preferível, mesmo que isso signifique minimizar discussões sobre responsabilidades.

Portanto, a autenticidade é essencial para garantir que uma pessoa seja reconhecida corretamente como ela mesma, evitando o acesso indevido ou atividades mal-intencionadas.

INTEGRIDADE

O conceito de integridade, quando aplicado moralmente, refere-se a possuir bons valores. Na Segurança da Informação, especificamente, significa assegurar que a informação não seja alterada indevidamente.

Para ilustrar isso, apresentam-se dois personagens: Zezinho e Marieta. Supõe-se que Zezinho envie um texto para Marieta com a palavra “Bogo!”. Quando Marieta recebe o texto, ele chega exatamente da mesma forma, sem ter sofrido nenhuma modificação. Isso demonstra que a integridade foi mantida.

Se o texto, por exemplo, chegasse a Marieta sem a exclamação, apenas como “bogo.”, isso representaria uma alteração e haveria perda da integridade da informação.

A garantia que se busca é que o texto chegue sem alterações no meio do caminho. Um exemplo disso é o ataque do “homem no meio” (man in the middle), em que um agente intercepta a informação, a modifica e a envia de forma diferente para o destinatário. Isso pode ser comparado à dinâmica do “telefone sem fio”, em que uma informação é distorcida ao ser passada adiante. Embora o telefone sem fio às vezes seja apenas uma questão de má interpretação, pode também ocorrer de forma intencional, distorcendo a informação original.

Portanto, garantir a integridade significa assegurar que a informação mantenha sua forma original desde sua origem até seu destino. Esse conceito será explorado mais a fundo posteriormente, mostrando como garantir a integridade e sua correlação com outros aspectos da segurança da informação.

DISPONIBILIDADE




Este conceito pode ser comparado aos relacionamentos interpessoais. Quando se está com alguém, espera-se que essa pessoa esteja disponível em diversos momentos, seja durante um dia ensolarado, uma noite de lua cheia ou até mesmo em situações adversas, como uma tempestade. Portanto, qual é o conceito que se aborda para garantir a disponibilidade das informações?

As informações devem estar acessíveis às pessoas autorizadas sempre que necessário. Suponha que alguém tente acessar um banco de dados e, por alguma razão, com uma queda de energia sem um backup de energia secundário, a informação não está disponível. Não importa qual seja a causa desse problema, o fato é que a informação não está acessível quando deveria estar para uma pessoa autorizada.

25m

Se uma pessoa for a uma agência depois das 20 horas e tentar sacar, poderia dizer que o serviço não estava disponível para ela? Não. Isso porque é preciso considerar o horário em que o saque era permitido. Das 8 da manhã às 20 horas. Após as 20 horas, não era esperado que estivesse disponível, então não se pode falar em perda de disponibilidade.

Disponibilidade é a garantia de que a informação estará acessível para as pessoas autorizadas a qualquer momento. Em situações extremas, como um furacão, a disponibilidade pode ser comprometida, já que não é possível garantir o funcionamento em meio a uma tempestade severa, na qual a energia pode falhar.

GABARITO

1. a
2. d