Livro Eletrônico

Trilha Estratégica

Trilha 06

Banco do Brasil (Escriturário-Agente Comercial) Trilha Estratégica 2021 (Pós-Edital)

Professor: Luis Eduardo, Renan Peron Fineto, Lucalio Almeida Elmiro, Camila de Fátima Campos Damázio

13.4 30

Estratégia Concursos

TRILHA ESTRATÉGICA PÓS-EDITAL PARA O BANCO DO BRASIL ESCRITURÁRIO – AGENTE COMERCIAL

Olá, alunos(as)!

Sejam muito bem-vindos à ***Trilha Estratégica Pós-Edital para o Banco do Brasil – Escriturário (2021)***. Chegamos à sétima semana de estudos, sendo a esta a nossa ***Trilha #06***. Neste ciclo iremos finalizar o estudo de duas disciplinas. Vamos avançar!

Fonte: Correio Braziliense

Não deixem de participar de nosso canal no ***Telegram***. O link está logo adiante. Se surgir alguma ***dúvida***, ou se você detectar alguma ***inconsistência*** na trilha, ficaremos muito gratos se você nos avisar. O formulário para tal fim você também encontrará na próxima página.

Um abraço e bons estudos.

Contem comigo!

Lucailo Elmiro

@proflucailoelmiro

1 – Comunidade de Alunos

Para que os alunos possam receber dicas constantes e rápidas, nós temos a ***Comunidade da Trilha Pós-Edital BB 2021***.

Consiste em um canal no ***Telegram*** no qual você pode fazer a inscrição clicando no link azul logo abaixo:

Baixe o aplicativo no seu celular, cadastre-se no Telegram e, então, clique no link abaixo para se juntar à Comunidade de Alunos:

https://t.me/joinchat/aK_unvDnD5QwY2Ix

Escolhemos o aplicativo do ***Telegram*** em virtude de diversos recursos que não temos no ***WhatsApp***. Ela é a única plataforma que preserva a intimidade dos assinantes e que, além disso, possui recursos tecnológicos compatíveis com os objetivos da nossa Comunidade de Alunos.

Você pode usar o ***Telegram*** seguramente pelo aplicativo no seu celular ou direto pelo computador. Basta fazer o download do aplicativo no seu aparelho ou então acessar no computador através do link a seguir:

https://web.telegram.org/

Mas é importante fazer o cadastro no ***Telegram*** antes de clicar no link para se juntar à ***Comunidade de Alunos***. Caso contrário, dará erro nesse procedimento, ok?

Espero você lá no ***Telegram***!

2 – Dúvidas

Para que os alunos possam enviar suas ***dúvidas*** relativas à Trilha, criamos o Formulário abaixo:

http://estrategi.ac/r4a478

Importante: as respostas serão enviadas através da nossa ***Comunidade do Telegram***. Portanto, a sua participação é muito importante!

TRILHA ESTRATÉGICA 06

Ciclo de Estudos

Lembre-se que a ideia da trilha pós-edital é criar um arcabouço teórico que irá subsidiar essa jornada de estudos de **13 semanas**. Além disso, tentaremos criar essa base da forma mais eficiente possível, trabalhando as matérias na sequência que acreditamos ser a mais saudável para o aluno.

Chegamos à **sétima semana** de estudos. Neste ciclo, iremos finalizar as disciplinas de **Inglês** e **Atualidades do Mercado Financeiro**. E, atendendo a alguns pedidos, e visando dar a preparação mais consistente possível para vocês, iremos disponibilizar duas trilhas alternativas para os estudos das disciplinas de **Conhecimentos Bancários** e de **Atualidades do Mercado Financeiro** pelos cursos do Prof. Celso Natale disponíveis na área do aluno.

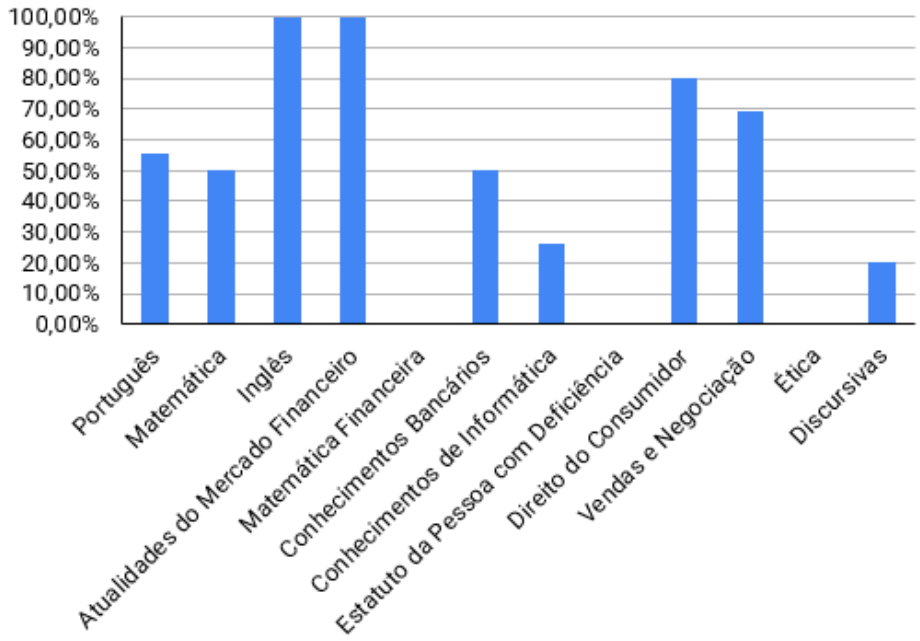
Atenção: as trilhas de disciplinas alternativas para essas duas matérias são uma sugestão e uma possibilidade a mais para **aprofundamento** e **revisão**. Você não precisa abandonar o curso regular da trilha, que está utilizando o curso da Profª. Amanda Aires (principalmente se está gostando da abordagem dela). Você poderá encontrar o link para as trilhas alternativas dessas matérias (que serão disponibilizadas ao longo da semana) na lista de trilhas de disciplinas adiante.

Assim, para este ciclo com as seguintes disciplinas:

- **Português;**
- **Conhecimentos Bancários;**
- **Matemática;**
- **Informática;**
- **Atualidades do Mercado Financeiro;**
- **Inglês;**
- **Vendas e Negociação.**
- **Direito do Consumidor; e**
- **Discursivas.**

As demais disciplinas serão adicionadas ao ciclo de estudos ao longo das nossas Trilhas.

O gráfico abaixo demonstra a nossa evolução nas matérias até aqui:



Com relação ao tempo, estimamos um **tempo médio de 1h30** para que o aluno iniciante execute cada tarefa desta Trilha. Cabe ressaltar que é apenas uma estimativa. O que o aluno deve fazer é prezar pela qualidade do estudo, nunca pela quantidade ou pela velocidade de assimilação.

Por último, comunico que as Trilhas serão, em sua maioria, pautadas na leitura dos arquivos em **PDF**. A tarefa o indicará qual o melhor material a utilizar para aquele assunto ou revisão (PDF completo, resumido ou marcado pelos aprovados). Como estamos na fase pós-edital, **não** é aconselhável que você perca tempo assistindo as videoaulas. Siga à risca o que pede a tarefa e mantenha a atenção nos materiais escritos.

Sem perder tempo, vamos começar!

Trilhas de Disciplinas

Disponibilizaremos individualmente, nesta seção, as Trilhas de cada uma das disciplinas trabalhadas por nós. O objetivo é que o aluno possa fazer ajustes no seu estudo a depender do nível em que ele está em determinada matéria.

Matéria	Trilha de Disciplina
Português	http://estrategi.ac/hrmfie
Matemática	http://estrategi.ac/kktzb6
Inglês	http://estrategi.ac/7y8r19
Atualidades do Mercado Financeiro	http://estrategi.ac/b8qvqe
Atualidades do Mercado Financeiro (Prof. Celso Natale)	http://estrategi.ac/52cmbg
Matemática Financeira	http://estrategi.ac/xuuv31
Conhecimentos Bancários	http://estrategi.ac/yk4iv9
Conhecimentos Bancários (Prof. Celso Natale)	http://estrategi.ac/3vngip
Conhecimentos de Informática	http://estrategi.ac/bkew0p
Estatuto da Pessoa com Deficiência	*Em breve*
Direito do Consumidor	http://estrategi.ac/f94gfu
Vendas e Negociação	http://estrategi.ac/xufmb1
Ética	*Em breve*
Discursivas	http://estrategi.ac/9qg7m9

Lembrando que aulas utilizadas como base para nossa trilha serão integralmente as do **Pacotaço - Pacote Teórico + Pacote Passo p/ Banco do Brasil (Escriturário - Agente Comercial) - 2021 - Pós-Edital**.

Link do Pacote:

https://www.estrategiaconcursos.com.br/app/dashboard/pacote/171918/

TAREFA 119

Português

Revisão da aula 5: resolução de uma bateria do Sistema de Questões.

Nesta tarefa, iremos resolver uma bateria do Sistema de Questões sobre o tema que foi abordado na aula citada.

Utilize esse caderno como extensão da teoria, tendo muita atenção aos comentários das questões.

Observe sobre o que versam as questões que você errou e reforce tais conceitos por meio do seu material teórico e de revisão que construiu ao longo do seu estudo.

Segue caderno do Sistema de Questões sobre ***Sintaxe*** para resolução.

Link: *http://questo.es/4pr2h7*

Bons estudos!

TAREFA 120

Conhecimentos Bancários

Estudo da Aula 05 – PDF original, tópico "Mercados e Fundos de Investimento".

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171723/aulas/1468252/*

Nesta tarefa, vamos ater à última parte da aula 05, que trata do assunto Mercados e Fundos de Investimento. Abaixo, são listados os pontos os quais julgamos relevantes serem captados na sua leitura:

➲ saber diferenciar ***mercado primário*** de ***mercado secundário***;

➲ saber os conceitos de mercado de bolsa, mercado de balcão organizado e mercado de balcão não-organizado;

➲ como se dá o processo de distribuição de valores mobiliários (oferta primária e oferta secundária). Muito cuidado no conceito de ***underwriting***. **#Vaicair!**

➲ o que são entidades administradoras de mercados organizados de valores mobiliários. Perceba que o texto menciona no plural, ou seja, podem existir mais de uma entidade administradora no país;

➲ que a principal bolsa de valores citada na aula é a BM&F-BOVESPA, porém importante saber que atualmente a razão social é ***B3 S/A*** (*https://bit.ly/3yzMsjI*);

➲ a importância da ***autorregulação*** para a dinâmica de mercado atual, quais as ***características*** que precisa ter a entidade administradora para regular um determinado setor (autonomia administrativa e financeira) e quais ***penalidades*** a autorregulação pode aplicar.

Terminada a leitura do PDF, você pode aproveitar para ***refazer*** as questões que errou nas tarefas passadas e ***reler*** os comentários do professor das 30 questões ao final da aula. Na próxima tarefa, revisaremos todo o conteúdo de Mercado de Capitais.

TAREFA 121

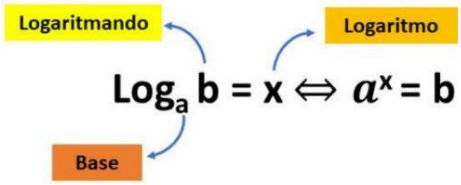
Matemática

Estudo da aula 09 (Função Logarítmica); e resolução de 10 questões.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171714/aulas/1469161*

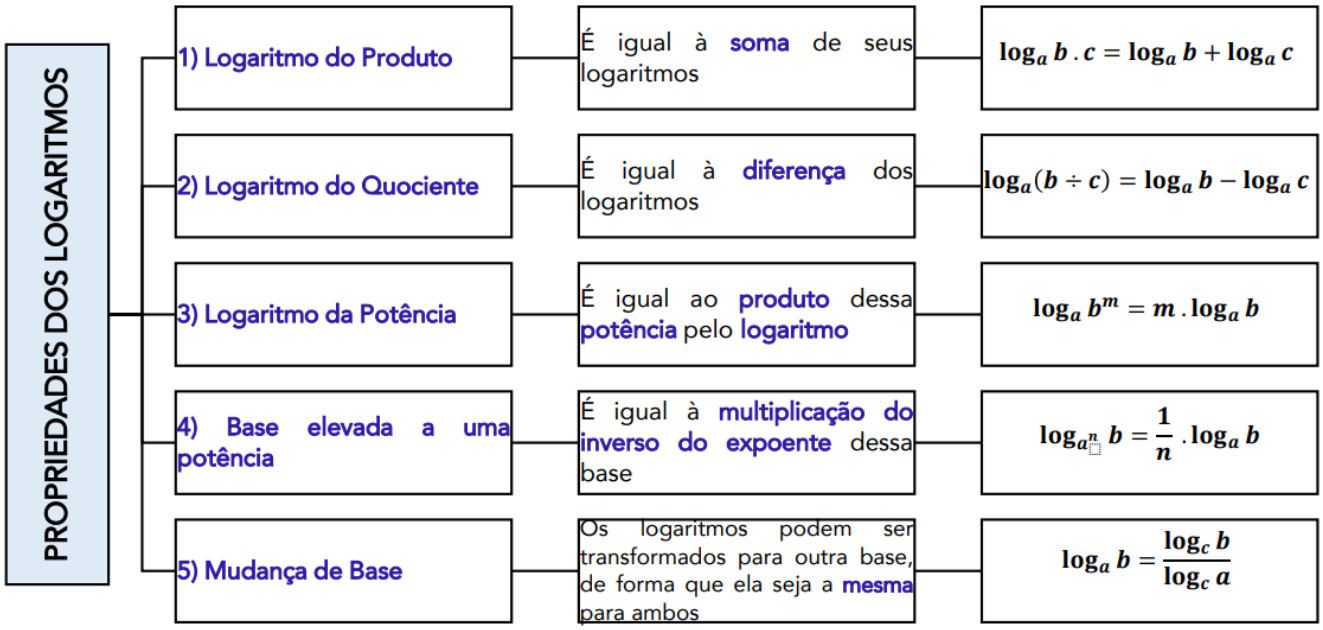
Essa aula traz um assunto muito temido no Ensino Médio. Para conseguir resolver as questões de logaritmo, você PRECISA decorar os conceitos iniciais e propriedades. Se você não fizer isso, será impossível evoluir nessa parte.

O primeiro ponto que devemos conhecer são os conceitos iniciais sobre Logaritmo, assim como o nome dado a cada uma de suas partes, conforme abaixo:



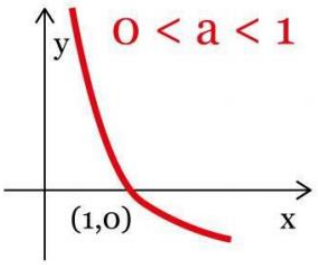
Na grande maioria das vezes, os exercícios de logaritmos são resolvidos com as técnicas que aprendemos em Equações Exponenciais, em que as bases devem ser igualadas, e resolvida a parte restante.

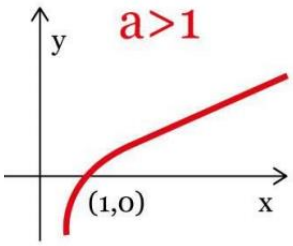
Decore as ***Propriedades do Logaritmos***:



Para resolver as questões de ***Equações Logarítmicas***, é necessário saber os conceitos de Logaritmos que aprendemos, em que o valor da "base" elevado ao logaritmo" é igual ao logaritmando. Eu recomendo que você analise alguns exemplos feitos pelo professor, eles vão ajudar demais.

Em relação aos ***gráficos da função*** $f(x) = \log_a x$, ela pode ser uma curva crescente (quando a base do logaritmo é maior que 1), ou uma curva decrescente (quando a base é um valor entre 0 e 1), conforme abaixo:





A seguir, resolva as questões ***1, 2, 3, 4, 5, 6, 7, 8, 9*** e ***10*** da aula através da lista sem comentários ao final do PDF. Após, recorra ao comentário do professor naquelas que errar ou ficar em dúvidas, marcando-as para futuras revisões.

TAREFA 122

Informática

Estudo da aula 05 - "Correio Eletrônico"; e resolução de 20 questões do PDF.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171724/aulas/1468499*

Nesta tarefa, quero que você:

1. Revise/Estude a teoria da aula e faça as questões que surgirem ao longo a explanação da parte teórica; e

2. Depois de estudada/revisada a parte teórica, vá para "Questões Comentadas – FCC" e resolva 05 (cinco) questões do PDF, conforme lista a seguir: 01, 06, 10, 18, 20 e 22; e

3. Depois de resolvidas as questões acima, vá para "Questões Comentadas – DIVERSAS BANCAS" e resolva 15 (quinze) questões do PDF, conforme lista a seguir: 07, 13, 16, 20, 24, 31 a 40.

Quanto à parte teórica, os principais pontos são:

1. ***Aspectos Gerais***

O Correio Eletrônico (Eletronic Mail ou E-Mail) é um método que permite compor, enviar e receber ***mensagens assíncronas*** através de sistemas eletrônicos de comunicação. Mensagem assíncrona é uma comunicação desconectada do tempo, isto é, emissor e receptor podem se comunicar à medida que tenham tempo disponível (Ex: Whatsapp). Em contrapartida, a comunicação síncrona exige que emissor e receptor estejam disponíveis simultaneamente (Ex: Telefone). No caso do Correio Eletrônico, emissor e receptor precisam apenas se conectar brevemente a um servidor de e-mail pelo tempo que for necessário para enviar ou receber mensagens.

2. ***Requisitos fundamentais***

Para utilizar um serviço de correio eletrônico, existem dois pré-requisitos básicos: (1) você deve possuir uma conta cadastrada em algum Provedor de E-Mail; (2) você deve utilizar uma ferramenta de correio eletrônico como um Cliente de E-Mail ou um Webmail. Vamos entender alguns conceitos:

- Provedor de E-Mail: trata-se de uma empresa que hospeda e disponibiliza serviços de e-mail para outras empresas ou usuários finais (Ex: Gmail, Outlook, Yahoo, Uol, etc).

- Provedor de E-Mail: trata-se de uma empresa que hospeda e disponibiliza serviços de e-mail para outras empresas ou usuários finais (Ex: Mozilla Thunderbird, Microsoft Outlook, etc).

- Webmail: trata-se de uma aplicação que hospedada em um servidor web remoto que permite enviar/receber e-mails (Ex: Outlook.com, Gmail.com, Yahoo.com, Uol.com, etc).

3. ***Etiqueta na Rede***

O conjunto de normas de conduta utilizadas no cotidiano para conduzir melhor as relações e comunicações humanas na internet é conhecido como ***Netiqueta***.

Existem algumas recomendações de etiqueta para correio eletrônico, entre elas:

-Evite utilizar letras maiúsculas – elas geralmente significam falar alto ou GRITAR.

-No envio de e-mail para diversas pessoas, é recomendado utilizar o recurso da cópia oculta.

4. ***Sintaxe dos endereços***

Um e-mail válido possui três partes, quais sejam: Nome do Recipiente, Símbolo de Arroba e Nome do Domínio.

- Nome do Recipiente: também chamado de ***Nome da Conta de Usuário*** ou ***Parte Local***, representa a conta de e-mail de um receptor qualquer.

- Símbolo de Arroba: trata-se de um símbolo (**@**) que separa o Nome do Recipiente do Nome do Host/Domínio – é obrigatório que haja necessariamente uma, e apenas uma, ocorrência desse símbolo no endereço.

- Nome do Domínio: também chamado de ***Nome de Host*** ou ***Nome do Provedor***, trata-se da identificação de um dispositivo que disponibiliza ou hospeda (host) algum serviço.

Lembre-se que o domínio pode possuir subdomínios: em ***estrategiaconcursos.com.br***, temos um domínio de nível mais baixo ***estrategiaconcursos***; um domínio de segundo nível com e um domínio de topo ***br***.

5. ***Assinatura de E-Mail***

Esse recurso permite que informações de contato, endereço, cargo, saudações, entre outros possam ser inseridas no corpo do e-mail de forma automática ao final da mensagem.

6. ***PROTOCOLOS DE E-MAIL***

Um Servidor de E-Mail é uma máquina que envia, recebe e armazena e-mails para usuários. No caso de Servidores de E-Mail, há três protocolos que podem ser usados: ***POP3, SMTP e IMAP.***

6.1 ***SMTP (SIMPLE MAIL TRANSFER PROTOCOL)***

Trata-se do protocolo responsável pela transmissão de correio eletrônico pela internet. Por padrão, ele roda na Porta ***TCP 25***. No entanto, ele vem sendo substituída no Brasil pela Porta 587.

6.2 ***POP3 (POST OFFICE PROTOCOL, VERSÃO 3)***

Protocolo criado como uma forma simplificada de receber, baixar e deletar mensagens de um servidor de e-mail – funciona na Porta ***TCP 110***.

Esse protocolo trabalha em dois modos distintos: ou ele apaga as mensagens da caixa postal logo após a realização do download; ou ele mantém uma cópia das mensagens na caixa postal mesmo após a realização do download.

6.3 ***IMAP (INTERNET MESSAGE ACCESS PROTOCOL)***

Protocolo que – em contraste com o POP3 – não apaga as mensagens da caixa de correio – elas ficam permanentemente armazenadas no servidor. Funciona na Porta ***TCP 143*** ou 993 (SSL/TLS).

7. ***PASTAS***

Os serviços de correio eletrônico permitem a utilização de ***pastas*** e ***subpastas*** para organizar as mensagens das caixas de correio de seus usuários. Iremos ver as principais pastas a seguir.

7.1 ***Caixa de Entrada***

Trata-se de uma pasta que armazena mensagens de e-mail recebidas e são organizadas, em geral, por remetente, assunto e data de recebimento.

7.2 ***Caixa de Saída***

Trata-se de uma pasta que armazena temporariamente as mensagens pendentes de envio.

7.3 ***Itens Enviados***

Trata-se de uma pasta que armazena mensagens de e-mail enviadas/transmitidas com êxito e são organizadas, em geral, por destinatário, assunto e data de envio.

Fique atento com a diferença entre ***Caixa de Saída e Rascunho***. A primeira apresenta mensagens que foram escritas, enviadas pelo usuário, mas que ainda estão em processo de envio pelo servidor; já a segunda apresenta mensagens que foram escritas, mas ainda não foram enviadas pelo usuário.

7.4 ***Lixo Eletrônico***

Também chamada de ***Spam***, trata-se de uma pasta que armazena mensagens identificadas como spam.

7.5 ***Itens Excluídos***

Também chamada de ***Lixeira***, trata-se de uma pasta que armazena mensagens que foram excluídas de outras pastas, mas que ainda não foram eliminadas em definitivo.

7.6 ***Rascunho***

Trata-se de uma pasta em que são armazenadas mensagens que ainda estão sendo redigidas e preparadas para serem enviadas posteriormente.

8. ***ENVIO DE E-MAIL***

8.1. ***De***

Trata-se do remetente da mensagem, isto é, a entidade que está enviando um correio eletrônico para uma ou mais entidades.

8.2. ***Para***

Trata-se do destinatário da mensagem. Em geral, quando há mais de um, basta utilizar ponto-e-vírgula (;) no preenchimento dos endereços. A entrega de e-mails ao destinatário não é garantida, uma vez que sua caixa de entrada pode estar lotada, pode haver destinatários em excesso, o endereço de destino não existe ou está incorreto, entre outros.

8.3. ***Assunto***

Trata-se do assunto da mensagem que será enviada. Atente-se, pois esse é um campo de preenchimento ***facultativo***, ou seja, você não é obrigado a preenchê-lo.

8.4. ***Com Cópia (Cc)***

A etiqueta da internet considera que – caso o endereço de e-mail de uma pessoa esteja no campo de destinatário – espera-se alguma resposta dela. Se não for necessária nenhuma resposta, isto é, apenas deseja-se dar ciência a essa pessoa, é uma boa prática colocá-la em cópia e, não, como destinatária principal da mensagem.

8.5. ***Com Cópia Oculta (Cco)***

Também conhecido como Blind Carbon Copy – ***Bcc***, esse recurso tem o objetivo de ocultar os destinatários em cópia.

8.6. ***Confirmação de Entrega/Leitura***

Uma Confirmação de Entrega confirma a entrega de seu e-mail na caixa de correio do destinatário, o que não significa que o destinatário o viu ou o leu. A Confirmação de Leitura confirma que sua mensagem foi ao menos aberta pelo destinatário – mesmo que não signifique que ele tenha lido a mensagem.

Perceba que não há nenhuma maneira de forçar obrigatoriamente um destinatário a enviar uma confirmação de leitura caso ele não queira.

8.7. ***Anexo***

Recurso que permite que qualquer arquivo (documento, imagem, texto, vídeo, etc) enviado ao destinatário seja incorporado a uma mensagem de correio eletrônico.

9. ***RESPOSTA DE E-MAIL***

9.1. ***Responder (a Todos)***

Responder a um e-mail é geralmente o próximo passo ao dar seguimento ou se comunicar com o remetente sobre um assunto em particular. Quando for utilizado o recurso "***Responder***" apenas o remetente originário da mensagem recebe uma resposta. Já quando é utilizado "***Responder a todos***" a resposta será encaminhada para o destinatário principal e aos destinatários secundários.

9.2. ***Encaminhar***

Funcionalidade de enviar uma mensagem de e-mail recebida geralmente para outros destinatários que não estavam na lista de remetentes ou em cópia na mensagem.

Atenção! Ao responder mensagens com anexo, eles não são anexados; já ao encaminhar mensagens com anexos, eles são anexados.

10. ***WEBMAIL***

Webmail é uma forma de acessar o serviço de correio eletrônico através da web, utilizando para tal um navegador e um computador conectado à Internet. Em um webmail, todas as mensagens ficam armazenadas em pastas no Servidor de E-Mail e, não, na máquina do usuário – em contraste com os Clientes de E-Mail.

TAREFA 123

Atualidades do Mercado Financeiro

Resolução de exercícios sobre os assuntos da Aula 03 por curso alternativo

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171755/aulas/1468557*

Vamos continuar exercitando e, dessa forma, aumentar as nossas possibilidades. Aproveitando o PDF da aula 03 do professor **Celso Natale**, resolva todas as questões comentadas ao final do referido PDF (***1*** a ***25***). Deixe para conferir pelos comentários do professor somente após tentar resolver sozinho(a) a lista inteira!

Mãos à obra!

TAREFA 124

Discursiva

Estudo da aula 01, do tópico 6 ao 12, inclusive.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171760/aulas/1468611*

Antes de mais nada, você deve ter atenção sempre que o professor colocar os quadros "Resumindo", "Atenção Decore", "Tome Nota" e "Esta cai na prova". São assuntos que o próprio professor já está classificando como importantes.

O tópico 6 traz os tipos de argumentos que o aluno pode utilizar na construção de um texto dissertativo. Tenha atenção ao assunto, pois uma boa argumentação costuma ser o diferencial em provas discursivas.

Saiba diferenciar tema, tese e assunto. Aproveite os exemplos dados pelo professor.

Tema: Delimitação do assunto sobre o qual irá escrever.
Tese: Ponto de vista, sua opinião sobre o tema.
Assunto: Generalização do tema.

Tenha bastante atenção ao desenvolvimento por explicação/fundamentação. Essa forma é uma das mais simples e a mais utilizada. Nesse tipo de desenvolvimento, a fundamentação para cada tópico solicitado no enunciado é exposta em um parágrafo. Observe bem os exemplos trazidos pelo professor para que você não fique com dúvidas.

Saiba bem as diferenças entre os fechamentos reforço, avanço e expansão:

Fechamento reforço: Reforça o ponto de vista apresentado na introdução.
Fechamento avanço: Indica um caminho para solucionar a problemática exposta.
Fechamento expansão: Estabelece a conexão com o último parágrafo do desenvolvimento para promover o fim da discussão.

No tópico 12, o professor traz alguns protótipos estratégicos de questões. Então, faça uma leitura atenta e vá internalizando os tipos de padrões.

TAREFA 125

Inglês

Revisão da aula 05; e resolução de 5 questões comentadas restantes. Resolução de 31 exercícios do Estratégia Questões.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171715/aulas/1468186*

REVISAR aula ***05*** pelo tópico: "RESUMO DA AULA", utilize-o como guia para revisar os pontos mais importantes da aula e/ou outros assuntos que você sinta necessidade; Tabela de "VOCABULÁRIOS", use-a para identificar palavras que precisam ir para o seu próprio DICIONÁRIO (essencialmente as palavras relacionadas com o cargo/carreira da prova e atualidades).

RESOLVER as ***5*** questões "não resolvidas" da aula.

SEMPRE faça as questões, inicialmente, sem olhar a resposta. Após, leia os comentários dos professores e, se achar necessário, volte ao conteúdo da aula ou ao seu dicionário para rever "algo" que você perceba que ainda está "fraco".

FAZER ainda o seguinte caderno EQ, ***31*** questões, ÁREAS AFINS, CESGRANRIO:

http://questo.es/iq0phb

Antes de "partir" para as questões, volte nas DICAS dos professores para leitura e interpretação de textos que foram colocadas em TAREFAS anteriores. Aproveite-a ou use-a para montar a sua própria. Assim como metodologia de estudo, metodologia para resolver questões é fundamental para resolver provas de concurso.

Venho insistindo nesse ponto desde as primeiras TAREFAS. Pois bem, o motivo dessa insistência é simples, SEM TÉCNICA DE RESOLUÇÃO DE QUESTÕES HÁ UMA TENDÊNCIA MAIOR DE ERRAR POR BOBEIRA, mesmo para quem é fluente em inglês. Não quero ouvir você ao final da conferência do gabarito dizer…"essa eu errei de besteira, puts!"

FAÇA todas SEM VER OS COMENTÁRIOS (ao final da aula tem as questões sem comentários). Só depois volte na parte comentada para tirar as dúvidas.

Ao final, RELEMBRE seu DICIONÁRIO PARTICULAR.

TAREFA 126

Direito do Consumidor

Resolução de 22 questões da aula 04.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171726/aulas/1470020*

Inicie esta tarefa fazendo uma breve revisão teórica da aula. Na sequência, resolva questões ***1 a 22*** da aula.

Sugiro que você resolva as questões pela lista com comentários, leia com atenção antes de marcar o gabarito e só então veja a resposta. Isso vai ajudá-lo a ir se apropriando do conteúdo. Depois, leia os comentários do professor e grife o que julgar importante.

E não esqueça de deixar assinaladas as questões que você errar, ou responder com dúvida. Elas serão muito úteis nas revisões.

TAREFA 127

Vendas e Negociação

Resolução de 63 questões da aula 09; e leitura do resumo estratégico da aula 08.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171742/aulas/1468375*

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171742/aulas/1468374*

Vamos agora resolver todas as ***63*** questões da aula 09 para verificar a assimilação dos assuntos da tarefa anterior.

Após a resolução das questões, faça uma leitura do **resumo estratégico** da aula 08 (PDF Simplificado) com foco nos principais pontos que o(a) fizeram errar as questões.

Não se esqueça de marcar as questões que errou ou acertou sem ter certeza, para realizá-las novamente em futuras revisões.

TAREFA 128

Português

Estudo da aula 6, do tópico "Considerações Iniciais" até o tópico "O uso da Vírgula" - PDF Simplificado; e resolução de 17 questões.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171713/aulas/1468536*

Inicialmente, cumpre salientar que os alunos que já dominam o assunto da respectiva aula podem ir direto para as questões e revisar os pontos que identificarem dificuldades nos exercícios indicados ao fim desta tarefa.

Caso não domine os assuntos abordados nesta aula, tome por base o PDF Simplificado, tendo especial atenção aos tópicos abaixo destacados.

Nessa aula, passaremos ao estudo dos sinais de *pontuação*, que também costumam ter uma incidência relevante em provas das principais bancas, inclusive a CESGRANRIO.

O professor inicia a aula discorrendo sobre 2 princípios básicos acerca do uso da *vírgula*! É importantíssimo que o aluno entenda cada um, afinal, conforme veremos, o uso da vírgula é observado em diversas situações, o que dificulta o processo de memorização. Então, o entendimento de tais princípios básicos possibilita o aluno de acertar questões sobre o tema, sem ter que lembrar exatamente das regras específicas acerca do uso da vírgula.

Adentrando, então, nas regras específicas sobre o uso da vírgula, é importante ter em mente, além dos 2 princípios básicos, o seguinte: "Esqueça aquela história de que a vírgula é para respirar ou para fazer pausas. A vírgula é essencialmente um marcador de funções sintáticas." O que isso significa? Bem, significa que o uso ou a omissão da vírgula altera sintática ou semanticamente o texto. Pelos exemplos trazidos pelo professor, isso fica muito claro!

São muitas as situações em que a vírgula é usada, não é verdade!? Bem, pode parecer assustadora a ideia de que se precisa decorar todas essas situações, mas não se preocupem, afinal, essa ideia não é verdadeira. Lembram que comentamos sobre a importância dos 2 princípios básicos? Pois é, com eles é possível resolver a maioria das questões sobre o uso da vírgula! Vamos dar um exemplo!

"Vou estudar português na biblioteca." Essa frase precisa de vírgula? NÃO! E como podemos ter tanta certeza? A frase está na ordem direta, logo não podemos separar os termos! É um dos princípios básicos, lembram?

Agora vamos modificar um pouco a frase: "Vou estudar, na biblioteca, português." Dessa vez precisamos da vírgula, afinal o termo "na biblioteca" no meio da sentença passa a ideia de esclarecimento! Logo, percebemos a aplicação do segundo princípio básico!

Conhecendo, portanto, os princípios básicos, não é preciso lembrar que a vírgula deve ser utilizada para separar adjunto adverbial deslocado, por exemplo.

Resolver as questões ***1*** a ***17***, que surgem no decorrer da teoria.

TAREFA 129

Conhecimentos Bancários

Revisão da Aula 05; e resolução de 21 questões do SQ.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171723/aulas/1468252/*

Aproveite este momento para revisar os assuntos trazidos na ***Aula 05.*** Alguns tópicos estudados no PDF original são bem relevantes e bem passíveis de serem cobrados na prova, como Ações, Companhias (registro, divulgação de informações e operações de reorganização) e Mercado Primário e Secundário.

Após a leitura dos seus grifos e marcações, dirija-se até o ***Resumo*** disposto em forma de tópicos no final do PDF. Ele o(a) ajudará a memorizar o que foi estudado.

Feito isso, resolva o caderno de questões abaixo como forma de consolidação dos conhecimentos adquiridos sobre Mercado de Capitais:

Link: *http://questo.es/yrfvcr*

TAREFA 130

Matemática

Estudo da aula 05, do tópico "Conceito" até o tópico "Transformação de uma Fração Ordinária em Taxa Percentual", inclusive; e resolução de 10 questões.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171714/aulas/1469158*

Nesta aula iremos estudar ***Porcentagem***, um assunto superimportante, e com boa incidência em provas de concurso.

A primeira coisa que precisamos ter em mente sobre porcentagem é que ela pode ser representada de três formas diferentes: ***Forma Percentual*** (20%); ***Forma Fracionária*** (20/100); e ***Forma Unitária ou Decimal*** (0,20).

b

Em "***Cálculo da Porcentagem de um número***", o mais importante é saber que o termo "***de***" representa, em matemática, uma multiplicação. Assim, por exemplo, para calcular 30% ***de*** 450 é equivalente a calcular 30/100 ***x*** 450 = 135. É muito comum também utilizarmos Regra de Três para calcular o percentual de um número, em que o número total chamamos de 100%.

Já no tópico "***Transformação de uma Fração Ordinária em Taxa Percentual***", devemos ter em mente que para transformar uma fração em uma Taxa Percentual, precisamos multiplicar esta fração por 100 e, desta forma, já encontramos o resultado na forma percentual.

Nesta aula é muito importante acompanhar com bastante atenção a resolução de cada exercício e de cada exemplo trazido pelo professor. Desta forma, o aprendizado será muito mais consistente.

A seguir, resolva as questões ***4, 5, 10, 12, 14, 16, 20, 21, 24*** e ***28*** da aula através da lista sem comentários ao final do PDF. Após, recorra ao comentário do professor naquelas que errar ou ficar em dúvidas, marcando-as para futuras revisões.

TAREFA 131

Informática

Estudo da aula 06 - "Segurança da Informação"; e resolução de 20 questões do PDF.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171724/aulas/1468500*

Nesta tarefa, quero que você:

1. Revise/Estude a teoria da aula e faça as questões que surgirem ao longo a explanação da parte teórica; e

2. Depois de estudada/revisada a parte teórica, vá para "Questões Comentadas – FCC" e resolva 20 (vinte) questões do PDF, conforme lista a seguir: 06, 09, 10, 13, 16, 18, 20, 22, 24, 28, 29, 31, 33, 34, 37, 38, 40, 41, 42, e 43.

Quanto à parte teórica, os principais pontos são:

1. ***Aspectos Gerais***

A literatura acadêmica afirma que existe uma trindade sagrada da segurança da informação. São três princípios (também chamados de propriedades ou atributos): ***Confidencialidade, Integridade*** e ***Disponibilidade*** – conhecidas pela sigla ***CID***.

2. ***CONTROLES DE SEGURANÇA***

Os controles podem variar em natureza, mas – fundamentalmente – são formas de proteger a confidencialidade, integridade ou disponibilidade de informações. Em geral, eles são divididos em dois tipos:

- Controles Físicos: são barreiras que impedem ou limitam o acesso físico direto às informações ou à infraestrutura que contém as informações. Ex: portas, trancas, paredes, blindagem, vigilantes, geradores, sistemas de câmeras, alarmes, catracas, cadeados, salas cofre, alarmes de incêndio, crachás de identificação, entre outros.

- Controles Lógicos: também chamados de controles técnicos, são barreiras que impedem ou limitam o acesso à informação por meio do monitoramento e controle de acesso a informações e a sistemas de computação. Ex: senhas, firewalls, listas de controle de acesso, criptografia, biometria1, IDS, IPS, entre outros.

No que diz respeito às terminologias, perceba a diferença entre ***ameaça*** e ***risco***. A ameaça trata de um dano potencial, isto é, caso ocorra um incidente, poderá haver dano ou não. Já o risco trata de um dano real, isto é, caso ocorra um incidente, necessariamente haverá perdas ou danos.

3. ***PRINCÍPIOS FUNDAMENTAIS***

3.1. ***Confidencialidade***

Confidencialidade é a capacidade de um sistema de não permitir que informações estejam disponíveis ou sejam reveladas a entidades não autorizadas.

3.2. ***Integridade***

Integridade é a capacidade de garantir que a informação manipulada está correta, fidedigna e que não foi corrompida.

Perceba que a confidencialidade e integridade são princípios independentes, isto é, a quebra de um princípio não implica a quebra do outro.

3.3. ***Disponibilidade***

Disponibilidade é a propriedade de uma informação estar acessível e utilizável sob demanda por uma entidade autorizada. Ela garante que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Fique atento com esta ***PEGADINHA CLÁSSICA: CONFIDENCIALIDADE X DISPONIBILIDADE:*** A confidencialidade garante que a informação somente esteja acessível para ***usuários autorizados***. Já a disponibilidade garante que a informação esteja disponível aos ***usuários autorizados sempre que necessário***.

4. ***PRINCÍPIOS ADICIONAIS***

4.1. ***Autenticidade***

A autenticidade é a propriedade que trata da garantia de que um usuário é de fato quem alega ser. Desse modo, não confunda ***autenticidade*** com ***autorização***. A autenticidade busca garantir que a pessoa que está requisitando acesso a alguma informação é realmente quem ela diz ser. A autorização é o mecanismo que verifica se uma pessoa possui permissão para executar determinadas operações – esse não é considerado um dos princípios da segurança da informação.

4.2. ***Irretratabilidade***

Também chamada de Irrefutabilidade ou Não-repúdio, o princípio da irretratabilidade trata da capacidade de garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria.

5. ***CRIPTOLOGIA***

A Criptologia se ocupa da ocultação de informações e da quebra dos segredos de ocultação. A primeira pode ser alcançada por Esteganografia ou Criptografia, e a segunda pode ser alcançada por Criptoanálise.

6. ***ESTEGANOGRAFIA***

É uma técnica utilizada para esconder informações. Seu objetivo é que as informações sejam transmitidas de forma invisível, sem que possam ser capturadas ou monitoradas.

7. ***CRIPTOGRAFIA E CRIPTOANÁLISE***

A Criptografia é a técnica de tornar uma ***mensagem ininteligível***. Atualmente são empregadas técnicas de criptografias ***simétricas, assimétricas*** e ***híbridas***. Essas técnicas empregam dois fundamentos principais: substituição, em que cada elemento no texto claro é mapeado para outro elemento; e transposição, em que os elementos no texto claro original são reorganizados.

7.1. ***Criptografia Simétrica***

A Criptografia Simétrica implica o uso de uma ***chave secreta*** utilizada tanto para codificar quanto para decodificar informações. Ela garante apenas o princípio da confidencialidade e não é capaz de garantir o princípio da integridade, ou seja, que a mensagem não foi alterada no meio do caminho.

Principais algoritmos: DES, 3DES, AES, Blowfish, Cifragem de Júlio César, etc

7.2. ***Criptografia Assimétrica***

Criptografia Assimétrica também é chamada de ***Criptografia de Chave Pública.*** Nesse tipo de criptografia, nós possuímos ***duas chaves diferentes*** – uma ***chave pública*** e uma ***chave privada*** – por essa razão, é chamada de criptografia assimétrica. Esse par de chaves formam um par exclusivo, de modo que um texto criptografado pela chave pública só pode ser descriptografado pela chave privada e um texto criptografado pela chave privada só pode ser descriptografado pela chave pública. Nesse caso o Princípio da Confidencialidade é garantido, uma vez que somente o destinatário que possui a chave privada específica dessa chave pública conseguirá desfazer a operação de criptografia.

Se alguém utilizar a minha chave pública para descriptografar uma informação e conseguir, ela terá certeza de que fui eu que realmente criptografei aquela informação. Por quê? Porque se a informação foi descriptografada com minha chave pública, ela só pode ter sido criptografada com minha chave privada.

Principais algoritmos: RSA, DSA, ECDSA, etc.

7.3. ***Criptografia Híbrida***

Em geral, as chaves simétricas são bem menores que as chaves assimétricas. Dessa forma, a Criptografia Assimétrica chega a ser até cem vezes mais lenta que a Criptografia Simétrica. Por

essa razão, é comum a utilização de uma Criptografia Híbrida, ou seja, uma ***combinação*** da Criptografia Simétrica e Criptografia Assimétrica.

Basicamente, utiliza-se um algoritmo de Criptografia Assimétrica apenas para trocar chaves simétricas – chamadas de chaves de sessão – de forma segura. Protocolos como Secure Sockets Layer (SSL) utilizam chaves de sessão para criptografar e descriptografar informações.

8. ***Autenticidade***

Autenticidade é um dos princípios da Segurança da Informação. Podem-se utilizar diversos métodos de autenticação, inclusive uma combinação entre eles. Veremos abaixo os principais:

Método de Autenticação: O que você sabe?

Trata-se da autenticação baseada no conhecimento de algo que somente você sabe, tais como: senhas, frases secretas, dados pessoais aleatórios, entre outros.

Método de Autenticação: O que você é?

Trata-se da autenticação baseada no conhecimento de algo que você é, como seus dados biométricos. Exemplos: impressão digital, padrão de retina, reconhecimento de voz, reconhecimento facial, assinatura manuscrita (característica comportamental individual), etc.

A respeito da ***biometria***, ela utiliza características físicas únicas para verificar sua identidade. A mais famosa é a impressão digital, entretanto podemos ter acessos biométricos através do reconhecimento de voz, varredura de retina e até mesmo DNA!

Método de Autenticação: O que você tem?

Trata-se da autenticação baseada em algo que somente o verdadeiro usuário possui, tais como: celulares, crachás, Smart Cards, chaves físicas, tokens, etc. Esse tipo de método tipicamente requer a presença física do usuário.

Um ***Smart Card*** é um cartão inteligente. Trata-se simplesmente de um cartão de plástico contendo um microprocessador – um chip – que armazena informações eletrônicas sobre o usuário. Os ***tokens*** são objetos de autenticação. Podem servir para armazenar senhas aleatórias (One Time Password) ou podem conter um conector USB servindo como mídia criptográfica, armazenando informações sobre o usuário (Certificado Digital), assim como um Smart Card.

AUTENTICAÇÃO FORTE

Autenticação Forte é um tipo de autenticação que ocorre quando se utiliza pelo menos dois desses três métodos de autenticação. Um exemplo é a Autenticação em Dois Fatores (ou Verificação em Duas Etapas).

9. ***ASSINATURA DIGITAL***

Trata-se de um método de autenticação de informação digital tipicamente tratada como substituta à assinatura física, já que elimina a necessidade de ter uma versão em papel do documento que necessita ser assinado. Por meio de um Algoritmo de Hash, é possível garantir a integridade dos dados.

A Assinatura Digital garantirá a ***Autenticidade***, a ***Integridade*** e a ***Irretratabilidade***. Para descobrir como ela fará isso, precisamos entender o conceito de ***Algoritmo de Hash*** (ou Resumo).

O que é importante memorizar é que o algoritmo de hash basicamente recebe dados de entrada de qualquer tamanho e produz um dado de saída de tamanho fixo. Outra característica do Algoritmo de Hash é que dada uma mesma entrada, a saída sempre será a mesma. Porém, o Algoritmo de Hash tem um problema: diferentes entradas podem gerar a mesma saída – nós chamamos isso de colisão.

Nós já sabemos que – para garantir autenticidade – basta utilizar a Criptografia Assimétrica e cifrar a informação com a minha chave privada. Nós também sabemos que – para garantir a integridade – basta utilizar um Algoritmo de Hash. Então, combinamos essas duas estratégias para alcançar nosso objetivo da assinatura digital.

Principais algoritmos: SHA-1 (Hash de 160 bits), MD5 (Hash de 128 bits), etc

10. ***CERTIFICADO DIGITAL***

Certificado Digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável – chamada ***Autoridade Certificadora*** – e que cumpre a função de associar uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas com o intuito de tornar as comunicações mais confiáveis e auferindo maior confiabilidade na autenticidade. Ele é capaz de garantir a ***autenticidade, integridade*** e ***não-repúdio***, e até c***onfidencialidade***.

Vimos que a Assinatura Digital possui uma autenticação relativamente frágil, porque não é possível saber se a chave pública que foi utilizada é realmente de quem diz ser. Para resolver esse problema, é necessária essa terceira parte confiável - ***Autoridade Certificadora (AC) -*** que é uma entidade responsável por emitir ***certificados digitais.***

Para que a Autoridade Certificadora também seja confiável, sua chave pública deve ser amplamente difundida de tal modo que todos possam conhecer e atestar a sua assinatura digital nos certificados gerados. Nesse sentido, temos aquele cadeado no canto esquerdo da Barra de Endereço que significa que essa página web um canal de comunicação criptografado e seguro. Nesse contexto, perceba que em algumas situações, você tentará utilizar um site cujo certificado não é confiável e o navegador informará sobre esse risco.

Uma Autoridade Certificadora é também responsável por publicar informações sobre certificados que não são mais confiáveis. Sempre que ela descobre ou é informada de que um certificado não é mais confiável, ela o inclui em uma "Lista Negra", chamada de ***Lista de Certificados Revogados***

(LCR). A LCR é um arquivo eletrônico publicado periodicamente pela Autoridade Certificadora, contendo o número de série dos certificados que não são mais válidos e a data de revogação.

11. ***Infraestrutura de Chave Pública (ICP-Brasil)***

Trata-se de uma entidade pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas. O Certificado Digital funcionará como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação.

A principal função da ICP é definir um conjunto de técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública. A ICP brasileira é denominada ICP-Brasil.

- Autoridade Certificadora Raiz

Trata-se da primeira autoridade da cadeia de certificação. Compete a ela emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu. A AC-Raiz também está encarregada de emitir a Lista de Certificados Revogados (LCR).

- Autoridade Certificadora

Trata-se de uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais.

Ela cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves. Cabe também à Autoridade Certificadora emitir Listas de Certificados Revogados (LCR).

- Autoridade de Registro

Trata-se de uma entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Tem por objetivo o recebimento, a validação, o encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. Cabe mencionar que as Autoridades de Registro não emitem certificados digitais.

É importante ressaltar que existe um padrão para Infraestrutura de Chaves Públicas. O Padrão X.509 (Versão 3) especifica, entre outras coisas, o formato dos certificados digitais.

12. ***Tipos de Certificado***

Certificado de Assinatura Digital (A): reúne os certificados de assinatura digital, utilizados na confirmação de identidade na web, em e-mails, em Redes Privadas Virtuais (VPNs) e em documentos eletrônicos com verificação da integridade das informações.

Certificado de Sigilo (S): reúne os certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados relacionais, de mensagens e de outras informações eletrônicas sigilosas.

TAREFA 132

Vendas e Negociação

Estudo da teoria da aula 10.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171742/aulas/1468376*

A aula versa sobre ***Negociação***. A estratégia sugerida aqui é realizar uma leitura sem a preocupação de memorizar nada no primeiro momento. Vamos priorizar o entendimento. Aqui, temos uma aula bem curta repleta de conceitos teóricos na visão de alguns autores.

Atente-se aos seguintes pontos-chave:

1. Conceito de Negociação, por Chiavenato. Foque no quadro "resumindo".

2. Características principais da negociação.

3. Estrutura básica do processo de negociação.

4. Aspectos objetivos da negociação.

5. Aspectos subjetivos.

6. Cinco passos do processo de negociação.

7. Quadro esquematizado sobre as Características da negociação:

Características da negociação	Negociação Distributiva (Distribuidora)	Negociação Integrativa (Integradora)
Recursos disponíveis	Quantidade **fixa** de recursos para ser dividida entre as partes	Quantidade **variável** de recursos para ser dividida entre as partes
Motivações básicas (Motivações primárias)	Eu **ganho**, você **perde**	Eu **ganho**, você **ganha**
Interesses básicos (Interesses primários)	**Antagonismo** e **oposição** em relação ao outro	**Convergência, congruência** e **coerência** com o outro
Foco dos relacionamentos	**Curto prazo**	**Longo prazo**

Fonte: Adaptado de Chiavenato, 2015.

TAREFA 133

Português

Estudo da aula 6, do tópico "Uso do ponto e vírgula" até o tópico "Uso dos parênteses" - PDF Simplificado; e resolução de 10 questões.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171713/aulas/1468536*

Dando sequência ao estudo dos sinais de pontuação, nos deparamos com o *ponto e vírgula*. Sua definição clássica é ser uma pausa maior que a vírgula e menor que o ponto final, ou seja, é uma pontuação intermediária entre os dois. Sobre as regras específicas acerca da sua utilização, temos duas situações mais comuns: (i) antes de conectivos adversativos e conclusivos e (ii) para enumerar e agrupar elementos sem enumeração.

Sobre o sinal de *dois pontos*, por ora, lembrar que ele pode ser usado para (i) iniciar alguma citação ou enumeração, (ii) ligar orações ou termos que tenham natureza de "explicação" e (iii) isolar uma oração subordinada substantiva apositiva.

A princípio, tentem entender bem as situações por meio dos exemplos. Decorar cada uma dessas regrinhas não traz um ganho relevante, afinal, as questões de prova costumam questionar se determinada sentença está gramaticalmente correta, e não exigem o conhecimento de cada uma dessas regrinhas específicas.

Sobre as *reticências*, importante lembrar sempre que indicam uma interrupção de algo que ia continuar.

Já em relação às *aspas*, lembrar que podem ser utilizadas em quatro situações:

-Indicar citações diretas;

-Indicar sentido irônico, figurado ou impróprio de uma palavra;

-Destacar títulos, termos técnicos, expressões fixas, definições, exemplificações;

-Indicar gírias, neologismos, criações vocabulares não incorporadas à língua portuguesa.

Com relação ao uso do *travessão*, deve-se saber que ele é usado para indicar mudança de interlocutor e, em várias situações, pode funcionar como vírgula.

Por fim, temos os *parênteses*, que, aparentemente, têm a função mais fácil de ser identificada, dentre os sinais de pontuação estudados. Essencialmente, os parênteses servem para isolar esclarecimentos acessórios.

Resolver as questões 18 a 27, que surgem no decorrer da teoria.

TAREFA 134

Conhecimentos Bancários

Estudo da Aula 06 – PDF original, toda a teoria; e resolução de 07 questões.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171723/aulas/1468253/*

Na aula 06 iremos estudar o ***Mercado de Câmbio***. É um assunto de baixa incidência (**5,62%**) em provas anteriores da área bancária, mas podemos ser surpreendidos. Portanto, seguem alguns conceitos da aula para ficarmos ligados ao estudarmos o PDF.

De antemão, aprenda que o Mercado de Câmbio é o "m*ercado onde se realizam as* ***operações de compra e venda de moedas conversíveis*** *e ouro-instrumento cambial, entre residentes e não residentes.*"

Já no primeiro tópico, apreenda o conceito de Taxa de Câmbio, qual seja, o preço da moeda nacional em termos de moeda estrangeira. Ou seja:

$$E = \frac{R\$}{US\$}$$

No entanto, você perceberá que a taxa que mais interessa para nós a Taxa Real, que é aquela que mede a variação da taxa de câmbio considerando também a variação de preços interna e externa:

$$\theta = E \times \frac{Q}{P}$$

É muito importante que você compreenda o quadro "Se liga" da coruja. Nele, é descrita a variação na taxa de câmbio e o saldo do BP, a qual é fundamental para entender como a taxa de câmbio afeta as exportações e importações de uma economia.

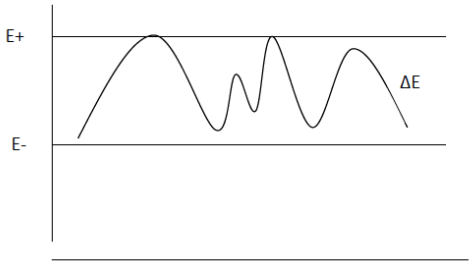
Prosseguindo no estudo, não deixe de entender os ***regimes de câmbio*** existentes:

(a) Câmbio Fixo; [*onde o preço do dólar é mantido artificialmente*];

(b) Câmbio Flexível; e [*o preço do dólar é livremente definido pela regra de oferta e demanda*];

(c) Regimes Intermediários. [*a autoridade monetária intervém no mercado para conter a volatilidade*];

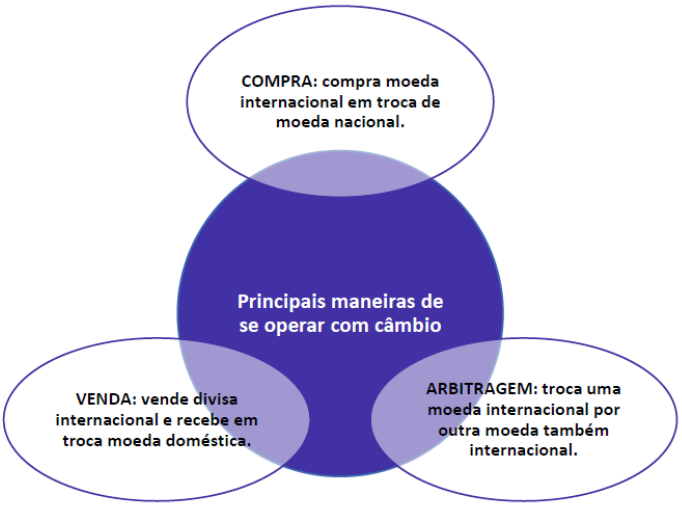
Nesse último tópico, tenha atenção ao regime de bandas cambiais e o seu característico gráfico exemplificativo (#VAICAIR):



Adiante, aprenda como as ***expectativas*** afetam os regimes de câmbio (fixo e flutuante). Esse tópico deve ser compreendido através dos exemplos dados pelo professor (você exportador e País 'A').

No tópico seguinte, memorize quais são os agentes ***autorizados*** pelo Banco Central do Brasil a realizar operações de câmbio. Importante que você memorize aqui quais operações cada IF pode efetivamente realizar **(#VAICAIR)**.

Adiante, em Principais Operações, aproveite o tópico para entender quais são as operações realizadas dentro desse mercado. É fundamental, inicialmente, que se compreenda as três principais maneiras de se operar com câmbio:



Adiante, aprenda as principais características das "***Operações Manuais"***, "***de Remessa"*** e de "***Contratos de Câmbio"***, pois podem vir como surpresinhas na prova.

Por fim, leia sem muitos aprofundamentos sobre "***Operações com Ouro***", "***SISCOMEX***" e "***Financiamento à importação e exportação com recursos do BNDES***", são temas não muito cobrados em provas de concursos públicos.

Vá até a Lista de Questões Comentadas (primeira lista) e resolva as questões ***1*** a ***7.*** Após a resolução, veja os comentários para entender melhor cada assertiva da questão.

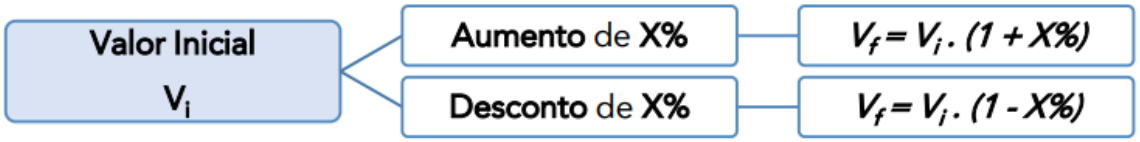
TAREFA 135

Matemática

Estudo da aula 05, do tópico "Aumentos e Descontos Percentuais" até o final; e resolução de 12 questões.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171714/aulas/1469158*

Continuando o estudo sobre ***Porcentagem***, vamos ver agora o tópico Aumentos e Descontos Percentuais, em que o mais relevante é compreender como estruturar a resolução de cada questão, além de memorizar as respectivas fórmulas, tanto no caso de reajuste, como no caso de desconto de valores:



Já no caso de ***aumentos e descontos percentuais sucessivos***, é fundamental compreender que, por exemplo, dois aumentos sucessivos de 20% cada, não representam um único aumento de 40%. Assim, faz-se necessário memorizar a seguinte fórmula, em que utilizamos o sinal de "+" nos casos de aumentos, e o sinal de "-" nos casos de descontos:

$$\mathbf{V_f = V_i . (1 \pm i_1) . (1 \pm i_2) . (1 \pm i_3) \ldots}$$

E no caso em que o enunciado pedir a taxa de ***aumento/desconto resultante***, devemos utilizar a seguinte fórmula, em que o sinal "**+**" representa um aumento, e o sinal "**-**" representa um desconto:

$$\mathbf{(1 + i_R) = (1 \pm i_1) . (1 \pm i_2) . (1 \pm i_3) \ldots}$$

Lembrando aquele detalhe que um aumento de $i\%$ e depois um desconto de $i\%$ ***não resulta no valor inicial.***

E quando um enunciado de prova fornecer o Valor Inicial e o Valor Final de um mesmo produto, e a seguir perguntar sua ***Variação Percentual***, vale a pena utilizar a seguinte fórmula abaixo:

$$\Delta\% = \frac{v_{final} - v_{inicial}}{v_{inicial}} \times 100$$

Dica: Aqui, caro aluno, o aprendizado da matéria virá com a resolução de muitas e muitas questões, de forma a fixar e reconhecer como o assunto costuma ser perguntado em prova, além de visualizar a forma de resolução de cada uma das questões. Desta forma, é muito importante prestar muita atenção nos exemplos apresentados pelo professor durante a explicação da matéria.

A seguir, resolva as questões ***1, 2, 3, 6, 7, 8, 9, 11, 13, 15, 17*** e ***23*** da aula através da lista sem comentários ao final do PDF. Após, recorra ao comentário do professor naquelas que errar ou ficar em dúvidas, marcando-as para futuras revisões.

TAREFA 136

Informática

Estudo da aula 07 - "Malwares"; e resolução de 20 questões do PDF.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171724/aulas/1468501*

Nesta tarefa, quero que você:

1. Revise/Estude a teoria da aula;

2. Faça as questões que surgirem ao longo da explanação da parte teórica; e

2. Depois de estudada/revisada a parte teórica, vá para "Questões Comentadas – DIVERSAS BANCAS" e resolva 20 (vinte) questões do PDF, conforme lista a seguir: 03, 09, 12, 15, 17, 18, 21, 23, 25, 27, 29, 30, 33, 34, 35, 37, 38, 40, 41 e 42.

Quanto à parte teórica, os principais pontos são:

1. ***Aspectos básicos:***

Malwares (Malicious Softwares) – também chamados de ***Softwares Maliciosos ou Pragas Virtuais*** – são programas especificamente desenvolvidos para ***executar ações danosas e atividades maliciosas em um computador***.

As formas mais comuns de infecção são:

• Pela exploração de vulnerabilidades existentes nos programas instalados ou pela auto-execução de mídias removíveis infectadas, como pen-drives;

• Pelo acesso a páginas maliciosas, utilizando navegadores vulneráveis ou pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

• Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas web ou de outros computadores.

Então, uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários.

O termo malware abrange ***qualquer tipo de software indesejado, instalado sem o devido consentimento no computador do usuário***.

As principais categorias de malwares são:

• Vírus;

- Worm;
- Bot;
- Trojan;
- Spyware;
- Backdoor;
- RootKit.

Já quanto aos ***procedimentos de segurança***, pode-se citar:

- Manter os programas instalados com as versões mais recentes;
- Ser cuidadoso ao instalar aplicativos desenvolvidos por terceiros;
- Utilizar apenas softwares originais (sem pirataria);
- Manter os programas instalados com todas as atualizações aplicadas;
- Utilizar mecanismos de proteção (antivírus, firewall, etc);
- Ser cuidadoso ao enviar seu computador para serviços de manutenção;
- Utilizar configurações de segurança disponíveis;
- Ser cuidadoso ao manipular arquivos;
- Proteger seus dados (utilizando backup, por exemplo);
- Manter seu computador com data e hora corretas;
- Criar um disco de recuperação de sistema;
- Ser cuidadoso ao utilizar o computador em locais públicos.

2. ***Terminologia***:

Hacker: Aquele que invade sistemas computacionais para provar sua capacidade e habilidades com computadores;

Cracker: Aquele que invadem sistemas para roubar informações e causar danos às vítimas e/ou decifra códigos indevidamente e destroe proteções de software favorecendo a pirataria;

Phreaking: É um especialista em telefonia;

Warez: Software pirata distribuído ilegalmente pela internet;

Spam: Termo usado para se referir aos e-mails não solicitados geralmente enviados para um grande número de pessoas com finalidade comercial.

*3.**Vírus:***

O vírus é um programa ou parte de um programa, normalmente malicioso, que se propaga infectando, ***inserindo cópias de si mesmo***, ***anexando-se ou hospedando-se em arquivos ou programas existentes na máquina***.

O principal objetivo de um vírus é replicar-se e contaminar o maior número possível de programas, de maneira a comprometer outros sistemas. Para tal, o vírus ***depende da execução do programa ou arquivo hospedeiro*** para se tornar ativo e dar continuidade à infecção.

Com isso, pode-se dizer, então, que um vírus realiza duas tarefas: primeiro, replica-se das mais variadas formas; segundo, executa seu código malicioso, podendo exercer diversas funcionalidades danosas na máquina infectada.

Composição do Vírus:

• ***Mecanismo de Infecção***: Meios ou formas pelas quais um vírus se propaga, habilitando-o a se reproduzir. É também conhecido como Vetor de Infecção;

• ***Mecanismo de Ativação***: Evento ou condição que determina quando a carga útil é ativada ou entregue. Às vezes, é conhecido como Bomba Lógica.

• ***Carga Útil***: O que o vírus faz, além de se espalhar. A carga útil pode envolver algum dano ou atividade benigna, porém notável.

Quando se trata de vírus de computador, eles podem ser classificados em quatro fases de execução:

Dormência: Nessa fase, o vírus está ocioso. A certa altura, ele será ativado por algum evento.

Propagação: Nessa fase, o vírus instala uma cópia de si mesmo em outros programas ou em certas áreas do sistema no disco.

Ativação: Nessa fase, o vírus é ativado para executar a função pretendida. Como ocorre com a fase de dormência, a fase de ativação pode ser causada por uma variedade de eventos de sistema.

Ação: Nessa fase, a função é executada. Ela pode ser inofensiva, como uma mensagem na tela, ou danosa, como a destruição de programas e arquivos de dados.

Importante:

Todo Sistema Operacional (SO) pode ser alvo de vírus

3.1) ***Vírus de Script***:
Um ***script é um conjunto de instruções que devem ser executadas***, a título de exemplo, pode-se citar os documentos do Excel, os quais podem possuir as famosas ***macros***, que são basicamente scripts que executam alguma funcionalidade no documento.

Em suma, vírus de script são softwares maliciosos que podem ser escritos em alguma linguagem de script (Ex: JavaScript ou VBScript).

3.2) ***Vírus de Macro***:
Os vírus de macro são um tipo específico de vírus de script – escrito em linguagem de macro – que tenta infectar arquivos manipulados por aplicativos que utilizam essa linguagem como, por exemplo, os ***arquivos de dados que compõem o Microsoft Office*** (Excel, Word, PowerPoint, Access, entre outros).

Os vírus de macro utilizam ***técnicas de propagação baseadas em anexos*** de documentos que executam macros, uma vez que os usuários frequentemente compartilham documentos com recursos de macro habilitados.

3.3) ***Vírus de Boot***:
O Vírus de Boot – também chamado de Vírus de Setor ou Vírus de Setor de Inicialização – infecta a parte de ***inicialização do sistema operacional***, escondendo-se no primeiro setor da memória.

Ele é ***ativado quando o computador é ligado*** e é carregado na memória antes mesmo do carregamento do sistema operacional. Salienta-se que a ***formatação rápida*** de um pendrive infectado ***não garante a remoção completa de vírus***, uma vez que alguns malwares conseguem se alojar na MBR (Master Boot Record) – que é o setor de inicialização de dispositivos de armazenamento.

3.4) ***Vírus de Arquivo***:
Também chamado de Vírus de Programa ou Vírus Parasitário, trata-se do vírus mais tradicional no cotidiano das pessoas. Ele ***infecta arquivos executáveis*** (.EXE, .VBS, .COM, .CMD, .PIF, .SYS, .SRC, .BAT, .HLP, .ASP e .REG), sobrescrevendo o código original e causando danos quase sempre irreparáveis.

3.5) ***Vírus Polimórfico***:
Também chamado de Vírus Mutante, é capaz de ***assumir múltiplas formas a cada infecção*** com o intuito de burlar o software de antivírus, ou seja, são capazes de criar uma nova variante a cada execução, alterando tanto a rotina de encriptação quanto a rotina de decriptação.

Uma variação do vírus ***polimórfico*** é o vírus metamórfico que, diferentemente do vírus polimórfico – se reescreve completamente a cada infecção, podendo mudar seu tamanho e comportamento, aumentando a dificuldade de detecção.

3.6) ***Vírus Stealth***:
Também chamado de Vírus Furtivo, eles são ***projetados explicitamente para não serem detectados pelo antivírus***, possuindo a ***capacidade de se remover da memória do computador*** temporariamente para evitar que o antivírus o detecte.

3.7) ***Vírus Time Bomb***:
Também conhecido como Vírus Bomba Relógio, trata-se de um vírus que – após infectar a máquina – permanece latente (oculto), apenas se replicando. Além disso, seu código malicioso ***é programado para ser ativado em um determinado momento específico, executando sua carga útil***.

4) ***Worm***:

Worm (ou Verme) ***é um programa*** capaz de se replicar automaticamente, enviando cópias de si mesmo de computador para computador. Diferente dos vírus, ele não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos através da rede, mas – sim – ***pela exploração automática de vulnerabilidades*** existentes em programas instalados em computadores ou pela execução direta de suas cópias.

5) ***Bot e Botnet***:

Bot é um programa que dispõe de mecanismos de ***comunicação com o invasor*** que permitem que ele seja controlado remotamente. Já uma Botnet ***é uma rede formada por centenas ou milhares de computadores zumbis*** e que permitem potencializar as ações danosas executadas pelos bots.

6) ***Trojan Horse***:

O Trojan Horse – também chamado de Cavalo de Troia – é um programa que, além de executar as funções para as quais foi aparentemente projetado, também ***executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário***.

7) ***Spyware***:

Um spyware ***é um software espião***, capaz de violar a privacidade das informações de usuários, coletando dados da máquina ou da rede e disponibilizando-as a terceiros.

8) ***Backdoor***:

Backdoor (em português, Porta dos Fundos) é um programa que ***permite o retorno de um invasor*** a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

9) ***Rootkit***:

Rootkit é um conjunto de programas e técnicas que ***permite esconder e assegurar a presença de um invasor*** ou de outro código malicioso em um computador comprometido. É muito importante ressaltar que o nome rootkit não indica que os programas e as técnicas que o compõem são usadas para obter acesso privilegiado a um computador, mas sim para mantê-lo.

10) ***Ransomware***:

O Ransomware é um tipo de código malicioso que ***torna inacessíveis os dados armazenados em um equipamento***, geralmente utilizando ***criptografia***, e que exige pagamento de um resgate (ransom, em inglês) para restabelecer o acesso ao usuário – trata-se de uma espécie de extorsão virtual.

- ***Ransomware Locker***: impede que você acesse o equipamento infectado.
- ***Ransomware Crypto***: impede que você acesse dados no equipamento infectado.

Esse segundo tipo utiliza criptografia para impedir que o usuário tenha acesso aos dados.

11) ***Keyloggers***:

Keylogger é um tipo de ***spyware*** capaz de capturar e ***armazenar as teclas digitadas pelo usuário no teclado do computador e enviá-las a um invasor***.

12) ***Screenloggers***:

Trata-se também de um ***spyware*** – similar ao keylogger – capaz de ***armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado***, ou a região que circunda a posição onde o mouse é clicado.

13) ***Adwares***:

Trata-se de um ***spyware*** projetado especificamente para ***apresentar propagandas***.

É um programa executado de forma automática e ***geralmente instalado sem o consentimento do usuário durante a instalação de outro software***.

14) ***Sniffer***:

É um ***analisador de pacotes de dados***, capaz de monitorar, interceptar e registrar tráfego de dados em segmentos de rede de computadores.

Ele é utilizado de forma ***legítima*** por administradores de redes, para ***detectar problemas***, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados. Ele também pode ser utilizado por ***atacantes***, para ***capturar informações sensíveis***, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de ***conexões inseguras***, ou seja, sem criptografia.

15) ***Bombas Lógicas***:

Trata-se de um software malicioso normalmente ***instalado por um usuário autorizado***, como um administrador da rede, que o mantém no sistema deixando-o programado para causar danos (como excluir arquivos importantes) em um determinado evento.

16) ***Exploits***:

Trata-se de uma ferramenta criada por hackers para permitir ***explorar vulnerabilidades*** ou brechas de segurança conhecidas de sistemas e assim permitir que atacantes possam ***praticar ações de invasões sem conhecimentos avançados***.

17) ***Hijacker***:

Trata-se de uma praga virtual que ***assume o controle do navegador*** e muda a forma como seu conteúdo é exibido quando você está navegando na web.

18) ***Ataques e Golpes:***

18.1) ***Engenharia Social***:

A ***Engenharia Social*** é uma técnica por meio da qual ***uma pessoa procura persuadir outra a executar determinadas ações por má-fé***. Ela é utilizada para ***obter informações*** importantes do usuário, ***através de sua ingenuidade ou da confiança***.

18.2) ***Força Bruta***:

Um ***Ataque de Força Bruta*** (Brute Force) consiste em adivinhar, por ***tentativa e erro***, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Um ataque de força bruta, dependendo de como é realizado, ***pode resultar em um ataque de negação*** de serviço, devido à sobrecarga produzida pela grande quantidade de tentativas realizadas em um pequeno período de tempo.

18.3) ***Denial Of Service (DoS)***:

Negação de serviço (Denial of Service – DoS) é uma técnica pela qual um ***atacante busca retirar de operação um serviço, um computador ou uma rede conectada à Internet***. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (Distributed Denial of Service – DDoS).

O objetivo destes ataques não é invadir nem coletar informações, mas – sim – exaurir recursos e causar indisponibilidades.

18.4) ***Ip Spoofing***:

O ***IP Spoofing*** (Falsificação/Mascaramento de IP) é uma técnica de invasão comumente empregada ***quando o mecanismo de autenticação de uma rede é baseado em endereços IP***.

18.5) ***E-Mail Spoofing***:

E-Mail Spoofing (Falsificação/Mascaramento de E-Mail) é uma técnica que consiste em ***alterar campos do cabeçalho de um e-mail***, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Essa técnica é possível devido a características do protocolo SMTP (Simple Mail Transfer Protocol) que ***permitem que campos do cabeçalho sejam falsificados***.

Ataques deste tipo ***são bastante usados para propagação de códigos maliciosos, envio de spam e em golpes de phishing***.

18.6) ***Phishing Scam***:

O Phishing Scam é uma fraude em que ***o golpista tenta enganar um usuário para obtenção de dados pessoais e financeiros*** que permitam a aplicação de um golpe, ***combinando técnicas computacionais e de engenharia social***.

São exemplos de Phishing Scam:

- Páginas falsas de comércio eletrônico ou Internet Banking;
- Páginas falsas de redes sociais ou de companhias aéreas.

18.7) ***Pharming***:

A tarefa do DNS é converter nomes de domínio em endereços IP, o que representa a localização real do site, permitindo que o navegador da Internet se conecte ao servidor em que o site está hospedado. O método mais comum de executar esse ataque é por meio do ***envenenamento de cache***.

Quando você digita o endereço de um site, seu navegador cria um cache (memória rápida) de DNS para que você não precise retornar ao servidor toda vez que quiser revisitar um site. ***O pharming é um tipo de phishing que "envenena" a tabela de cache do Servidor DNS***, corrompendo o servidor por meio da alteração de IPs e ***redirecionando o tráfego da Internet para sites fraudulentos para capturar informações e permitir a ação de golpistas***.

Em suma: pharming é um ataque que ***possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original***. É um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS.

18.8) ***Hoax***:

O ***Hoax (Boato) é uma mensagem que possui conteúdo alarmante ou falso*** e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.

18.9) ***Man in the Middle***:

O ***Man in the Middle*** é um ataque em que os dados trocados entre duas partes (Ex: você e o seu banco) são de alguma forma ***interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam***.

18.10) ***Defacement***:

Desfiguração de página (Defacement ou Pichação) é uma técnica que consiste em ***alterar o conteúdo da página web***.

TAREFA 137

Vendas e Negociação

Resolução de 16 questões da aula 10; e leitura do resumo estratégico.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171742/aulas/1468376*

Vamos agora resolver todas as ***16*** questões da aula 10 para verificar a assimilação dos assuntos da tarefa anterior.

Após a resolução das questões, faça uma leitura do resumo estratégico com foco nos principais pontos que o fizeram errar as questões.

Não se esqueça de marcar as questões que errou ou acertou sem ter certeza, para realizá-las novamente em futuras revisões.

TAREFA 138

Atualidades do Mercado Financeiro

Resolução de 26 questões do SQ sobre os assuntos estudados na Aula 03.

Vamos continuar exercitando e aumentando as nossas possibilidades. Resolva o caderno abaixo com 26 questões inéditas formuladas pela equipe do Estratégia sobre os assuntos estudados na Aula 03. Não se importe com o formato C/E. O importante é que você revise o consolide os conceitos aprendidos sobre *Marketplaces*, Arranjos de Pagamentos, *Pix* e Tranformação Digital no Sistema Financeiro.

Link: *http://questo.es/jyuqku*

TAREFA 139

Inglês

Estudo da aula 06, "Expressões Idiomáticas" até "Estrutura de Período Composto", inclusive; e de resolução de 20 questões comentadas.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171715/aulas/1468187*

ESTUDAR "Expressões Idiomáticas", você encontrará gírias e expressões que caso você não saiba o significado dificilmente você descobrirá através do contexto. Neste caso, dê ATENÇÃO às mais IMPORTANTES. Como saber quais? São aquelas que podem ter alguma relação com os assuntos afetos ao cargo que pretende ser aprovado. Não é fácil de "bingar", mas à medida que for avançando nas questões de prova a "mente abre"). ATENÇÃO ESPECIAL aos exemplos dos professores que dão uma noção exata de como os termos podem ser cobrados na prova.

Na sequência, ESTUDAR "Direct and Indirect Speech", não há regras para decorar. Uma leitura ATENTA já "mata" o tópico. Diferente do próximo tópico, "Numbers", DECORE os quadros apresentados. É um tópico importante para a prova, por vezes aparece em provas de inglês. Vale o custo-benefício, o MAPA MENTAL ao final do tópico vai auxiliar.

Para os TÓPICOS gramaticais seguintes, LEIA de forma ATENTA, mas não precisa se preocupar em gravar regras. Destes, dê mais ATENÇÃO: ao tópico "WH-QUESTIONS" que constantemente aparece em provas anteriores, por vezes, a cobrança deste tópico vem de forma isolada em uma pergunta.

Na sequência, RESOLVER as ***20*** questões relativas aos textos ***1 a 3***.

FAÇA a leitura do "GLOSSÁRIO DE TERMOS" e aproveite para identificar as palavras que precisam ir para o seu próprio DICIONÁRIO.

Ao final, RELEMBRE seu DICIONÁRIO e ***separe*** as palavras ainda ***não "fixadas"*** para que ***DIARIAMENTE*** você faça a REMEMORAÇÃO até a data da prova.

TAREFA 140

Direito do Consumidor

Resolução de 10 questões da aula 04.

Link: *https://www.estrategiaconcursos.com.br/app/dashboard/cursos/171726/aulas/1470020*

Inicie esta tarefa fazendo uma breve revisão teórica da aula. Na sequência, resolva as questões ***23 a 32***.

Sugiro que você resolva as questões pela lista com comentários, leia com atenção antes de marcar o gabarito e só então veja a resposta. Isso vai ajudá-lo a ir se apropriando do conteúdo. Depois, leia os comentários do professor e grife o que julgar importante.

Na sequência, refaça as questões desta aula selecionadas para revisão.

1. As Trilhas Estratégicas são meras ***sugestões*** de estudo com base em determinado objetivo (área de concurso, concurso específico ou perfil). O aluno deve ficar livre para que possa segui-la à risca ou fazer adaptações para o seu próprio estilo e rotina de estudo.
2. Os ***professores*** do Estratégia, ao elaborarem os seus materiais, possuem o objetivo de ensinar todo o conteúdo exigido pelo edital programático do concurso, além de estabelecer uma sequência ideal de estudo do ponto de vista pedagógico e considerando que o aluno terá tempo de estudar todo o seu material.
3. Já os ***coaches***, ao elaborarem as Trilhas Estratégicas, possuem o objetivo de fazer o aluno estudar o conteúdo de acordo com um determinado custo x benefício, porém muitas vezes fugindo da recomendação didática de estudo proposta pelos professores para que os alunos possam fazer um estudo direcionado.
4. Como dizemos sempre: *o ideal é estudar todos os assuntos, revisar tudo, fazer muitos exercícios de todos os assuntos e chegar na prova bom em todos os assuntos também*. Entretanto, são poucos aqueles alunos que dispõem de tempo para isso!
5. Nosso objetivo aqui é sugerir uma sequência de estudos baseada na **experiência de *coaches*** aprovados em diversos concursos para que possamos dar orientações e maiores chances de aprovação aos alunos.

Espero que tenha gostado!

Bons estudos!

Aguardo você no ***Telegram***.

"Todo progresso acontece fora da zona de conforto." (Michael John Bobak)

Lucailo Elmiro

@proflucailoelmiro

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.