Editora Solução
a solução para o seu concurso!

SABARÁ - MG

PREFEITURA MUNICIPAL DE SABARÁ - MINAS GERAIS

Agente Administrativo Escolar

EDITAL Nº 001/2023

CÓD: SL-077DZ-23
7908433246664

Língua Portuguesa

1. Leitura, compreensão e interpretação de textos e gêneros textuais diversos. 7
2. Vocabulário: sentido denotativo e conotativo, sinonímia, antonímia, homonímia, paronímia e polissemia. 8
3. Variantes linguísticas, linguagem oral e linguagem escrita, formal e informal e gíria. 8
4. Ortografia: emprego das letras e acentuação gráfica. 10
5. Fonética: encontros vocálicos e consonantais, dígrafos e implicações na divisão de sílabas. 12
6. Regras de acentuação gráfica. 14
7. Crase. 14
8. Pontuação: emprego de todos os sinais de pontuação 14
9. Classes de palavras: classificações e flexões. 16
10. Morfologia e flexões do gênero, número e grau. 21
11. Termos da oração: identificação e classificação. Processos sintáticos de coordenação e subordinação; classificação dos períodos e orações. 24
12. Concordâncias nominal e verbal. 29
13. Regências nominal e verbal. 30
14. Estrutura e formação das palavras 32

Matemática

1. Números inteiros: operações e propriedades. Números racionais, representação fracionária e decimal: operações e propriedades. Números reais: operações e propriedades 43
2. Razão e proporção. Regra de três simples. 52
3. Mínimo Múltiplo Comum e Máximo Divisor Comum: propriedades e problemas. Múltiplos e divisores de um número 54
4. Álgebra: expressões algébricas, frações algébricas 55
5. Monômios e polinômios: operações e propriedades. Produtos notáveis e fatoração 59
6. Equação de 1° grau e do 2° grau. Inequações do 1° e 2° graus. Sistemas de equações do 1° e 2° graus 63
7. Problemas que envolvem álgebra, equações, inequações e sistemas do 1° ou do 2° graus 69
8. Leitura de gráficos e tabelas 71
9. Média Aritmética e Ponderada 76
10. Funções: função afim, quadrática, modular, exponencial e logarítmica. Gráficos, propriedades e problemas envolvendo funções afim, modular, quadrática, exponencial e logarítmica 77
11. Sequências e Progressões: Progressão Aritmética e Geométrica. Propriedades e problemas envolvendo PA e PG. Soma dos termos de uma PA e uma PG 83
12. Sistema métrico: medidas de tempo, comprimento, superfície e capacidade 85
13. Relação entre grandezas: tabelas e gráficos 86
14. Raciocínio lógico 90
15. Resolução de situações problema 91
16. Geometria Plana: Angulos, retas paralelas, estudo dos polígonos e polígonos regulares. Triângulo: teoremas dos ângulos internos e externos. Estudo do triângulo retângulo; relações métricas no triângulo retângulo; relações trigonométricas (seno, cosseno e tangente); Teorema de Pitágoras. Quadriláteros: propriedades dos trapézios e paralelogramos. Círculo e circunferência: ângulos e propriedades. Áreas e perímetros de figuras planas e volume de sólidos. Poliedros, prismas e pirâmides: propriedades, áreas laterais e totais, volume e problemas. Relação de Euler. Corpos redondos: propriedades, áreas e volumes 95

17. Ciclo trigonométrico – trigonometria no círculo: funções trigonométricas 113
18. Sistemas Lineares, Matrizes e Determinantes. Operações, propriedades e problemas envolvendo sistemas lineares, matrizes e determinantes 115
19. Análise combinatória: princípio multiplicativo, permutações, arranjos e combinações. Problemas envolvendo análise combinatória 124
20. Probabilidade e Estatística 125
21. Números Complexos: operações e propriedades. 128
22. Matemática Financeira: Porcentagem, juros simples e compostos. Problemas envolvendo matemática financeira 129
23. Raciocínio lógico: diagramas lógicos. Conectivos e Tabelas verdade. Proposições e Silogismos 131
24. Correlacionamento de dados e informações. 138
25. Sequências não numéricas 143
26. Teoria dos Conjuntos 145

Conhecimentos Gerais / Legislação

1. Lei orgânica do Município 153
2. informações disponíveis sobre a cidade no site da Prefeitura 188
3. Atualidades do cenário nacional e internacional. Noções básicas sobre o País, o Estado e o Município referente: aspectos culturais, economia, educação, agricultura, pecuária, esporte, comércio e turismo 191
4. Noções de reciclagem e ecologia 191
5. Noções sobre primeiros socorros; primeiros socorros em caso de queimaduras, intoxicação, picadas de serpentes peçonhentas, picada de aranha, engasgo, fratura, desmaio, convulsão 198
6. Informática básica: noções de microcomputadores 205
7. sistemas operacionais: Microsoft Windows 206
8. Microsoft Office 97- 2003 ou superior. Word, Excel, Power Point 214
9. Internet 219

Informática

1. Conceitos básicos de operação de microcomputadores. Conceitos básicos de operação com arquivos em ambiente de rede Windows. Conhecimentos básicos e gerais de Sistema Operacional: Microsoft Windows, Microsoft Office 97- 2003 ou superior. Conhecimento de interface gráfica padrão Windows. Noções básicas de operação de microcomputadores e periféricos em rede local 227
2. Conceitos básicos para utilização dos softwares do pacote Microsoft Office, tais como: processador de texto, planilha eletrônica e aplicativo para apresentação e Excel. Word, Excel e PowerPoint 258
3. Conhecimento básico de consulta pela Internet e recebimento e envio de mensagens eletrônicas. Internet 280
4. Backup 286
5. Vírus 286
6. Ética profissional 288

Quando criança eu desenhava o mapa em folhas de papel almaço imaginando a beleza dos rios e lagos, a floresta densa, os cheiros da natureza, os mitos e as histórias dos que viviam entranhados nesse mundo mágico. Na fase adulta, posso ampliar essa acreanidade: sonho com um Acre amazônico por excelência, que se desenvolva valorizando suas tradições e tudo que a floresta nos ensinou e ensina."

As palavras MÁGICO e AMAZÔNICO estão corretamente acentuadas, já que ambas são:
(A) Paroxítonas terminadas em vogal.
(B) Oxítonas terminadas em vogal tônica.
(C) Paroxítonas.
(D) Proparoxítonas.
(E) Oxítonas no singular.

9. CRQ 9ª REGIÃO-PR — AUXILIAR ADMINISTRATIVO — FUNDATEC — 2018
Instrução: A questão refere-se ao texto abaixo. Os destaques ao longo do texto está citado na questão.

Contar mentirinhas vicia o cérebro, revela estudo
Por Felipe Germano Bruno Garatton

Mentir não faz o nariz crescer – mas pode ....., de outra forma, com o seu corpo. De acordo com um novo estudo realizado pela Universidade de Londres, contar mentirinhas leves provoca alterações físicas no cérebro, **que** se torna mais propenso __ optar por mentiras em momentos importantes.

Quando contam alguma mentira, as pessoas geralmente se sentem um pouco mal. Essa reação é provocada pela amígdala, uma região cerebral que também é ligada __ sensações de medo, e funciona como uma espécie de freio natural, limitando a quantidade de mentiras que as pessoas contam. Mas os cientistas descobriram que, se você contar uma sequência de pequenas mentiras, sem muita importância (na linha 'o seu penteado ficou ótimo' ou 'não vi o email'), esse freio vai ficando mais fraco.

Para calcular isso, os pesquisadores reuniram 80 voluntários e escanearam o cérebro deles enquanto eles jogavam um jogo. A brincadeira consistia em adivinhar quantas moedas havia em um pote e transmitir, por meio de um computador, a estimativa a outra pessoa. O jogo tinha várias modalidades. Numa delas, você era estimulado a dar uma 'mentidinha', superestimando a quantidade de moedas do pote, ... isso fazia você ganhar mais pontos, e a outra pessoa menos. Conforme o jogo avançava, os voluntários eram estimulados a mentir cada vez mais – e a atividade na amígdala se tornava cada vez menor. Era como se o cérebro estivesse se adaptando ao ato de mentir.

"A amígdala limita a ..... do quanto mentimos", diz a psicóloga Tali Sharot, líder do estudo. "Mas essa resposta vai diminuindo conforme as mentiras ficam maiores. Isso pode levar a uma reação em cadeia, em que pequenos atos de desonestidade acabam levando a mentiras maiores", acredita.

Para os pesquisadores, a capacidade que o cérebro tem de se acostumar não se aplica apenas __ mentiras. "Nós só testamos a desonestidade das pessoas nesse experimento, mas o mesmo princípio talvez seja aplicável a outras ações, como se expor __ riscos ou ter comportamentos violentos", afirma o cientista Neil Garrett, coautor do estudo.

(http://super.abril.com.br/comportamento/contar-mentirinhas-vicia-o-cerebro– Adaptação)

Em relação às letras e aos fonemas de palavras do texto, analise as afirmações que seguem e assinale C, se corretas, ou I, se incorretas.
( ) O vocábulo 'expor' é grafado com X, porém, esse fonema tem som de S. A palavra 'e_trair' segue a mesma grafia.
( ) A palavra 'consistia' tem o mesmo número de letras e fonemas.
( ) As palavras 'pequenos' e 'sequência' possuem dígrafos consonantais.
A ordem correta de preenchimento dos parênteses, de cima para baixo, é:
(A) C – C – C.
(B) C – C – I.
(C) I – C – C.
(D) I – I – I.
(E) C – I – I.

- Linha do Décio: (óculos) → não é vocalista e não tem 28 anos, logo quem usa óculos não tem 28 anos (informação já marcada).
- Linha do Roberto: (28 anos) → não é baterista, não é vocalista e não usa óculos, logo quem tem 28 anos não é baterista.

		Função				Idade				Item usado			
		BAT	GUIT	VOC	TEC	23	25	26	28	OCUL	BOT	GOL	GRAV
Nome	Benicio		N	N		N			N	N			
	Célia	N	N	S	N				N	N			
	Décio			N					N	S	N	N	N
	Roberto	N		N		N	N	N	S	N			
Item Usado	OCUL			N	N		N		N				
	BOT				N		N						
	GOL	N	N	N	S		N						
	GRAV				N	N	S	N	N				
Idade	23		N										
	25		N										
	26	N	S	N	N								
	28	N	N	N									

Observe que Na idade 28 anos sobrou apenas um espaço, sendo correspondente ao do Tecladista. Então o Tecladista tem 28 anos e Roberto tem 28 anos logo, Roberto é o Tecladista.

		Função				Idade				Item usado			
		BAT	GUIT	VOC	TEC	23	25	26	28	OCUL	BOT	GOL	GRAV
Nome	Benicio		N	N		N			N	N			
	Célia	N	N	S	N				N	N			
	Décio			N					N	S	N	N	N
	Roberto	N	N	N	S	N	N	N	S	N			
Item Usado	OCUL			N	N		N		N				
	BOT				N		N						
	GOL	N	N	N	S		N						
	GRAV				N	N	S	N	N				
Idade	23		N		N								
	25		N		N								
	26	N	S	N	N								
	28	N	N	N	S								

Nome	Função	Idade	Item usado
Benício			
Célia	Vocalista		
Décio			Óculos
Roberto	Tecladista	28	

Na dica 3, o que usou gravata tem 25 anos, e olhando na tabela gabarito acima, podemos concluir que Benício usou gravata.
Na dica 5, o tecladista usou gola de pele, descobrimos que Roberto usou gola de pele.
Como já sabemos também que Décio usou óculos, podemos concluir que só ficou
"Botas" para Célia.

Nome	Função	Idade	Item usado
Benício	Baterista	25	Gravata
Célia	Vocalista	23	Botas
Décio	Guitarrista	26	Óculos
Roberto	Tecladista	28	Gola

1º) Não se preocupe em terminar a tabela principal, uma vez que você tenha preenchido toda tabela gabarito. Ganhe tempo e parta para a próxima questão.

2º) Nunca se esqueça de que essa técnica é composta por duas tabelas que devem ser utilizadas em paralelo, ou seja, quando uma conclusão for tirada pelo uso de alguma delas, as outras devem ser atualizadas. A prática de resolução de questões de variados níveis de complexidade vai ajudá-lo a ficar mais seguro.

SEQUÊNCIAS NÃO NUMÉRICAS

A lógica *sequencial* envolve a percepção e interpretação de objetos que induzem a uma sequência, buscando reconhecer essa sequência e estabelecer sucessores a este objeto.

Muitas vezes essas questões vêm atreladas com aspectos aritméticos (sequências numéricas) ou geometria (construção de certas figuras).

Não há como sistematizar este assunto, então iremos ver alguns exemplos para nos *inspirar* para que busquemos resolver demais questões.

Exemplos:
1 – A sequência de números a seguir foi construída com um padrão lógico e é uma sequência ilimitada:

0, 1, 2, 3, 4, 5, 10, 11, 12, 13, 14, 15, 20, 21, 22, 23, 24, 25, 30, 31, 32, 33, 34, 35, 40, ...

A partir dessas informações, identifique o termo da posição 74 e o termo da posição 95. Qual a soma destes dois termos?

Vamos analisar esta sequência dada:
1º) Vemos que a sequência vai de 6 em 6 termos e pula para a dezena seguinte

Os primeiros 6 termos vão de 0 a 5
Do 7º termo ao 12º termo: 10 a 15
13º termo ao 18º termo: 20 a 25

2º) Vemos que o padrão segue a tabuada do 6

6 x 1 = 6 (0 até 5)
6 x 2 = 12 (10 até 15)
6 x 3 = 18 (20 até 25)

3º) O número que está multiplicando o 6 menos uma unidade representa a dezena que estamos começando a contar:

6 x 1 → 1 - 1 = 0 (0 até 5)
6 x 2 → 2 - 1 = 1 (10 até 15)
6 x 3 → 3 - 1 = 2 (20 até 25)

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de e-mail. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de pen-drives.

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:

– Vírus propagado por e-mail: recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado.

– Vírus de script: escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML.

– Vírus de macro: tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).

– Vírus de telefone celular: vírus que se propaga de celular para celular por meio da tecnologia bluetooth ou de mensagens MMS (Multimedia Message Service). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa.

Worm

Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

Bot e botnet

Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

Um computador infectado por um bot costuma ser chamado de zumbi (zombie computer), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de spam zombie quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio de spam.

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

Quanto mais zumbis participarem da botnet mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio bot), coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante (com o uso de proxies instalados nos zumbis).

Spyware

Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas. Pode ser considerado de uso:

– Legítimo: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

– Malicioso: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas spyware são:

– Keylogger: capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

– Screenlogger: 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.

– Adware: projetado especificamente para apresentar propagandas.

Backdoor

Backdoor 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.

Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Após incluído, o backdoor é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

utilizem senhas seguras com pelo menos um numeral e um símbolo ou letras maiúsculas e minúsculas e que elas sejam alteradas periodicamente.

Outra etapa requer certificar-se de que os funcionários não terão dificuldade em memorizar a senha, anotando-a e colocando-a em seu monitor ou escondendo-a embaixo do teclado ou numa gaveta da mesa de trabalho — lugares onde qualquer ladrão de dados experiente sabe que deve procurar primeiro. A boa prática de senha também requer que nunca se use a mesma senha ou senhas parecidas em mais de um sistema (MITINICK, 2005, p. 78).

SASSE e colaboradores (2001) ao abordar segurança da informação, referem-se ao usuário humano como sendo o elo mais fraco de um processo de segurança.

De acordo com MITNICK (2002):

Quando os empregados de confiança são enganados, influenciados ou manipulados para revelar informações sigilosas ou para executar ações que criem um buraco na segurança para que o atacante se infiltre, nenhuma tecnologia do mundo pode proteger uma organização.

De acordo com REZENDE e ABREU (2000), as organizações devem procurar dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório. Dessa forma, seria importante destacar que o elo mais fraco de um processo de segurança é a pessoa (ou grupos de pessoas), que por sua vez, é a responsável por garantir a fidelidade da informação.

Sob esta perspectiva, o usuário é vítima de alguém mal intencionado, mas será parte de um comportamento social avesso aos controles tecnológicos.

Ou seja, é uma ilusão imaginar que o uso de produtos de segurança padrão, da tecnologia da informação, torna as organizações imunes aos ataques.

As presentes definições nos conduzem ao entendimento do usuário como peça estratégica participante do processo interativo com sistemas de informação. Pode dizer que o usuário é todo aquele que produz, acessa, classifica, manuseia, transporta, transmite ou guarda informações organizacionais que possam ser alvo de ameaças.

Cultura Organizacional Relacionada com a Gestão da Segurança da Informação

WEBSTER (1995/1999, p. 6) aponta cinco definições para sociedade da informação, de acordo com os seguintes critérios: tecnológico, econômico, ocupacional, espacial e cultural. A definição mais comum da sociedade da informação tem ênfase na notável inovação tecnológica. O processamento, armazenamento e transmissão da informação levaram à aplicação da Tecnologia da Informação - TI - a todos os âmbitos da sociedade. Estamos em uma nova era, na qual os computadores estão mais eficazes, mais potentes, mais baratos, mais poderosos e com amplas aplicabilidades.

No entanto, de acordo com PROMON (2005, p. 4), os critérios da segurança da informação vão além da segurança lógica, permeando a importância da segurança física, cujo objetivo é a prevenção de acesso não autorizado a equipamentos e instalações, dano ou interferência às informações da organização. A estratégia organizacional é também uma forma de inserir a cultura organizacional nas atitudes dos administradores.

A cultura organizacional, como propriedade de uma unidade social formada por pessoas, deve conjuntamente buscar formas mais seguras que venham inibir condutas comportamentais que tornam o sistema de segurança vulnerável. SÊMOLA (2003, p. 17) alerta para o problema de que a equipe de segurança poderia estar não apenas voltada para aspectos tecnológicos da segurança, mas também deveria focar nos aspectos físico e humano.

A cultura organizacional é parte estratégica para o gestor que pretende tornar sua organização mais segura. A segurança depende do usuário, mas para que esse usuário torne-se peça colaboradora dos sistemas de segurança, a organização necessita incutir valores de segurança na cultura organizacional, pois assim o usuário pode tornar-se um colaborador inocente, comportando-se e agindo de forma segura. Os conceitos básicos de segurança precisam estar intrínsecos na cultura organizacional para que isso seja possível.

Definindo Políticas de Uso da Internet na Empresa[32]

Definir política de uso da Internet na empresa é mais do que uma recomendação, é uma necessidade: A Internet se tornou ao longo dos anos um valioso recurso no ambiente de trabalho, isso porque ela é a maior biblioteca de referência do mundo, lista telefônica, agenda de contatos, rede social e muito mais. Porém, quando mal utilizado, o uso da Internet pode prejudicar o trabalho e afetar drasticamente o desempenho dos resultados da empresa. Saiba o que você pode fazer para proteger sua empresa deste problema.

Os abusos no uso da Internet estão desde o assistente administrativo que gasta 3 horas por dia comentando nas fotos dos amigos no Facebook até o gerente do departamento que em sua sala acessa pornografia indiscriminadamente. Tipos de abuso frequentes são:

- Excesso/Abuso no uso de redes sociais (Facebook, Twitter, YouTube, etc);
- Acesso a pornografia e em casos mais extremos até mesmo conteúdo de pedofilia;
- Download de música/programas “piratas“;
- Streaming de música e rádios online;
- Bate papo e programas de comunicação instantânea (MSN, Skype, etc);
- Acesso a sites sem nenhuma relação com ambiente de trabalho (Fofocas, notícias de celebridades, receitas, etc);

Os itens acima podem oferecer complicações para a empresa e seus recursos das seguintes maneiras:

- Perda de produtividade / baixo desempenho;
- Problemas legais/jurídicos por conteúdo de pedofilia ou pirataria;
- Reduzir drásticamente a velocidade da Internet na empresa;
- Problemas com vírus, spyware e até roubo de informações da empresa;

Isso pode levar a problemas mais sérios caso não sejam administrados pontualmente, em alguns casos pode levar a demissão por justa causa, processos contra a empresa, problemas com segurança das informações e danos permanentes aos dados da empresa.

32 *Fonte: http://www.isengard.com.br/blog/definindo-politicas-de-uso-da-internet-na-empresa/*