

ANEXO XI - QUESTIONÁRIO TECNICO

O preenchimento deste questionário é obrigatório ao vencedor do processo de seleção.

As respostas serão analisadas pela Cbtarco em conformidade com as exigências técnicas e operacionais descrita no Edital e seus anexos e poderão ser auditadas em visita de diligenciamento.

O questionário deverá ser encaminhado no formato abaixo, ou seja, as respostas devem estar na mesma linha de cada questionamento.

Controle	Guia para Análises	RESPOSTA
Requisitos de Tecnologia		
1) Funcionários de TI	1. A empresa possui algum funcionário de TI? 2. Terceirizado ou CLT? 3. É fácil a comunicação entre o responsável de TI da empresa com os colaboradores do CBTARCO?	Sim, CLT e terceirizado
2) ISO 27001 - Gestão de segurança da informação ISO 22301 - Gestão de Continuidade de negócios.	1.1 - Proteção da informação contra vários tipos de ameaças de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno sobre investimentos e oportunidades de negócios. 1.2 - Para implantar a norma na empresa é obrigatório empregar todos os seus controles? Aplicam-se somente os controles para os serviços, facilidades, espaços e condições existentes na empresa. Por exemplo, se a empresa não tem acesso remoto de usuários, todos os controles referentes a esse tipo de acesso podem ser ignorados. 2.1 - Há algum Plano de Continuidade de Negócios / Plano de resposta a incidentes. A ISO 22301 especifica os requisitos para planejar, estabelecer, implementar, operar, monitorizar, rever, manter e melhorar continuamente um sistema de gestão, com o objetivo de responder eficazmente a ocorrências que possam interromper o normal funcionamento de uma organização. ***Ferramenta de gestão focalizada nos processos críticos da organização; ***Permite à organização reagir a grandes incidentes, através do estabelecimento de medidas adequadas; ***Minimiza perdas resultantes de rupturas ou avarias de processos cooperativos; ***Previne rupturas de processos críticos ao longo da cadeia de fornecimento; ***Melhora a compreensão holística da organização promovendo a melhoria contínua; ***Vantagens competitivas no mercado;	Isso trata-se de uma certificação que tem que ter. ISO 27001 é sobre governança e segurança dos dados de TI. A segunda trata-se de gestão contínua de negócio.

	***Evidência do cumprimento da legislação e regulamentos aplicáveis; ***Fornece uma base sólida para a negociação com prestadores de serviços financeiros; ***Aumento da confiança de todas as partes interessadas.	
3) O acesso a sistemas e aplicações críticas é restrito e disponibilizado apenas aqueles que são devidamente autorizados	1. Há Políticas, Norma ou Procedimentos relativos a gestão de acessos e perfis? 2. Os acessos a sistemas e aplicações críticas são revisados com qual periodicidade?	Todos os acessos e perfis de sistema são configurados e apenas acessados pelo responsável de TI. Sempre revisados semanalmente.
4) As informações contidas nos ativos liberados para trânsito são criptografadas.	1. A empresa disponibiliza ativos móveis para os funcionários? 2. Os ativos liberados para trânsito estão com as informações criptografadas (Ex: Notebooks, Smartphone, Tablets etc.)?	Sim. Todos os notebooks e celulares que os funcionários utilizam estão devidamente configurados para ter a maior segurança dos dados.
5) Há procedimentos específicos com os requisitos de segurança da organização para casos de roubo ou perda de recursos de computação móvel	1. Há Políticas, Norma ou Procedimento sobre como tratar roubo de ativos (Ex: Direitos Autorais em informações, fazer boletim de ocorrência na delegacia havendo roubo/furto de um ativo da empresa etc.)?	Temos um manual de procedimentos, assinados por todos os colaboradores
6) Há campanhas de conscientização e políticas de segurança da organização reforçando a necessidade de manter as informações críticas em sistemas ou na rede da empresa.	1. Há Políticas, Norma ou Procedimento informando que as informações críticas devem estar armazenadas em sistemas ou na rede da empresa (estas informações não devem estar apenas em dispositivos móveis ou no disco local)? 2. São realizadas campanhas de conscientização reforçando esta informação? Com qual periodicidade?	Sim. Todos os nossos colaboradores são treinados e utilizam servidores com firewall e nível de proteção dentro do ambiente corporativos apenas. Nenhuma informação crítica é fornecida externamente. Tudo se centraliza dentro da empresa.
7) Há segregação de função entre os profissionais que desenvolvem e os profissionais com autorização para incluir uma mudança no ambiente de produção.	1. Os profissionais com autorização para incluir uma mudança no ambiente de produção são diferentes dos profissionais responsáveis por realizar o desenvolvimento? 2. Os profissionais responsáveis pelo desenvolvimento possuem acesso lógico ao ambiente de produção?	Trata-se de diferentes funções e procedimentos implementados. Os profissionais que fazem as mudanças e criação de ambiente, são únicos. Existem diferentes equipes com nível de acesso para os procedimentos realizados. Os que fazem o desenvolvimento não tem acesso ao ambiente de produção.

8) Os dados armazenados de terceiros, clientes ou prestadores de serviço são devidamente destruídos, tendo sua confidencialidade assegurada por meio de procedimento de descarte de informações e cláusulas contratuais	1. Há alguma política e/ou procedimentos de descarte de informações de clientes, parceiros, fornecedores ou outros, mediante encerramento de contrato ou fim da relação corporativa? 2. De que forma o cumprimento destas normas são asseguradas? Há cláusulas contratuais que possam ser consideradas em suas relações comerciais ou parcerias?	Temos um manual de procedimentos, assinados por todos os colaboradores
9) Há política de descarte de dispositivos ou mídias de armazenamento, indicando os tratamentos nas informações antes de efetivar a destruição.	1. Há Políticas, Norma ou Procedimento de descarte de dispositivos e mídias de armazenamento? 2. Esta política indica o tratamento das informações antes de realizar a destruição (exemplo: deve ser analisado se há informações que não podem ser perdidas e devem ser armazenadas em outro local antes do descarte)?	Sim. Todos as plataformas de acesso de um colaboradores são revisadas pela equipe de TI e verificada a importância dos dados e fica a cargo de armazenamento dentro do servidores com firewall e nível de proteção da empresa.
10) Todos os equipamentos que contenham mídias de armazenamento de dados são examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança.	1. Há registros de descartes dos equipamentos? 2. Há registro da análise prévia dos dados armazenados nos equipamentos antes da realização da destruição?	Temos sim, encaminhamos para a empresa terceirizada que se responsabiliza em fazer o descarte, tudo devidamente documentado e assinado
11) Há campanhas de conscientização e políticas de segurança da informação indicando o tratamento e os cuidados necessários com os equipamentos da organização e as respectivas penalidades no caso de descumprimento.	1. Há Políticas, Norma ou Procedimento indicando o tratamento e os cuidados necessários com os equipamentos? 2. Há penalidades no caso de descumprimento deste item da política? 3. São realizadas campanhas de conscientização reforçando esta informação? Com qual periodicidade?	Existe sim normas e políticas de treinamento aos colaboradores de como utilizar de forma correta os dispositivos tecnológicos da empresa e a importância do bom funcionamento e das regras. Toda via nenhum sistema é instalado nos dispositivos sem autorização. Toda e qualquer instalação é feita unicamente pela TI da empresa. Nenhum funcionário exceto TI tem nível de acesso (bloqueado por senha), para instalar nenhum software.
12) São realizadas análises de vulnerabilidades dos aplicativos, sistemas operacionais e bancos de dados periodicamente.	1. São realizadas periodicamente análises de vulnerabilidades dos aplicativos, sistemas operacionais e bancos de dados? 2. Quem realiza as análises e qual a periodicidade? 3. Há tratamento e acompanhamento das	Sim. Além de termos licenças corporativas de antivírus nos dispositivos dos colaboradores, para análise imediata e

	vulnerabilidades identificadas?	prevenção de vulnerabilidade. Assim periodicamente a cada 15 dias fazemos a varredura e análise no sistema para prevenir ou identificar vulnerabilidades. Todo o tratamento e acompanhamento é feita exclusivamente pela equipe de TI.
13) Existem políticas, normas e procedimentos de Segurança da Informação amplamente divulgados.	1. Há política de segurança? 2. A política é divulgada para os funcionários? 3. Onde está localizada a Política (deve ser um local de fácil acesso aos funcionários)?	Sim. Há políticas de segurança e além de treinamento aos funcionários sobre tais políticas. Estamos sempre com os funcionários revendo procedimentos para não ocasionar erros.
14) Os acessos aos sistemas são concedidos após a solicitação e autorização formal e estes acessos são revisados periodicamente.	1. Há solicitação e autorização formal para acesso aos sistemas? 2. Há análise periódica dos acessos aos sistemas? Qual é a periodicidade e quem realiza? 3. Os acessos são revisados após alterações cargo/área? 4. Há análise da segregação de funções antes da liberação do acesso (exemplo: um profissional que solicita um pagamento não deve ter permissão para aprová-lo)?	Sim. Toda e qualquer solicitação de acesso é feita através do e-mail de suporte da empresa onde gera um ticket e fica registrado toda a solicitação. As análises são feitas a cada 15 dias nos sistemas, apenas pela equipe de TI. Todos os acessos são configurados e revisados em caso de mudança de cargo dos funcionários. A análise e configuração exata das funções de cada funcionário. Ex: O nível de acesso ao sistema de um emissor não é o mesmo de um funcionário do financeiro. Cada Funcionario tem um nível de acesso de acordo com seu cargo
15) Existência de um incentivo à conscientização das políticas de segurança, atendendo para a utilização de senhas fáceis, senhas guardadas perto do computador/sistemas, divulgação da senha a terceiros etc.	1. Existe um programa de conscientização de segurança? Está formalizado? 2. Os funcionários recebem treinamento sobre a política ? Com que frequência? 3. Como a eficácia do treinamento é avaliada?	Temos um manual de procedimentos, assinados por todos os colaboradores.

16) Os sistemas possuem senhas de acesso "fortes" e as senhas não são compartilhadas.	1. Todos os sistemas possuem senhas de acesso? 2. As senhas de acesso são "fortes" (formada por no mínimo 8 caracteres, com letras e números etc.)?	Sim. Todos os sistemas tem senhas fortes (letras, números e caracteres especiais) e não são compartilhadas.
17) Os funcionários são treinados sempre que um novo sistema é implementado ou alterado (alterações significativas).	1. Os funcionários são treinados sempre que novos sistemas são implementados? 2. Os funcionários são treinados sempre que alterações significativas são implementadas (alterações que mudem funcionalidades)?	Sempre que um novo sistema é implementado ou alterado, os funcionários são devidamente treinados.
18) Os acessos privilegiados são monitorados e os acessos são revisados periodicamente.	1. Os acessos privilegiados nos sistemas (SO e BD) são restritos e monitorados? 2. As senhas padrão dos usuários privilegiados foram alteradas? 3. Mesmo os usuários privilegiados possuem login e senha individuais? Os usuários privilegiados genéricos não são utilizados (exemplo root)? 4. Os acessos privilegiados são revisados periodicamente? Qual a periodicidade?	Sim. Todos os acessos com nível de privilégio são da TI. O usuário ROOT é desabilitado. E cada funcionário de TI tem sua própria senha com seus níveis de acesso e são revisados a cada 30 dias solicitando a troca das senhas.
19) Sistemas de segurança lógica para os sistemas.	1. Há sistema de segurança lógica para as aplicações (ex: Firewalls)? 2. As informações identificadas através do sistema de segurança lógica são tratadas? Há formalização destes tratamentos?	Sim. Utilizamos Firewalls dentro da empresa. Toda e qualquer informação de segurança é tratada pela TI.
20) Há procedimentos específicos informando as penalidades no caso de descumprimento da Segurança da Informação estabelecida para a empresa?	1. Há Políticas, Norma ou Procedimento indicando as penalidades no caso de descumprimento da Segurança da Informação estabelecida pela empresa? 2. As penalidades são aplicadas?	A segurança das informações e servidores tem normas e são obrigatoriamente cumpridas pelos funcionários responsáveis. Existem sim penalidades e se caso ocorrer alguma vulnerabilidade serão aplicadas sim.
21) Há procedimentos específicos ressaltando que as informações pessoais e da organização não devem ser fornecidas a desconhecidos, terceiros ou outros funcionários da empresa antes de entender o objetivo e antes de confirmar se possui esta autorização.	1. Há Políticas, Norma ou Procedimento indicando que as informações pessoais e da organização não devem ser fornecidas a desconhecidos, terceiros ou outros funcionários da empresa antes de entender o objetivo e antes de confirmar se possui esta autorização. 2. A conscientização sobre esta importância é realizada periodicamente? Qual a periodicidade?	A empresa faz treinamentos constantes sobre a importância da privacidade dos dados e informações. Todos os funcionários são conscientizados da importância de nunca fornecer nenhuma inf. a desconhecidos terceiros ou a qualquer pessoa que não tenha autorização.

22) Há controles de prevenção contra códigos maliciosos.	1. Há Políticas, Norma ou Procedimento proibindo o uso de softwares não autorizados? 2. Os profissionais possuem autorização para instalar quaisquer softwares em suas máquinas? 3. Caso necessite solicitar a TI a liberação para instalação de software, a TI analisa previamente os softwares antes de liberar? 4. Há softwares de controle de spam e phishing?	Sim. Todos os dispositivos possuem senha administrador, onde essa senha é a única que pode instalar software. Essa senha é de poderio único da equipe de TI. Nenhum colaborador tem esse nível de acesso. Nossos dispositivos possuem antivírus corporativo e sistema anti-malware, spam e phishing
23) Há softwares de detecção e remoção de códigos maliciosos.	1. Há atualização frequente de software de detecção de códigos maliciosos? (Ex: Antivírus) 2. Qual a periodicidade de realização?	Sim. Os nossos sistemas estão configurados para essa atualização 1 vez ao dia. E para detecção e bloqueio imediato
24) Há procedimentos específicos informando as penalidades no caso de ações realizadas propositalmente para desativar a infraestrutura/sistemas da empresa.	1. Há Políticas, Norma ou Procedimento indicando as penalidades no caso de ações realizadas propositalmente para desativar a infraestrutura/sistemas da empresa? 2. As penalidades são aplicadas?	Sim. Porém como todos os colaboradores recebem treinamento sobre esses procedimentos, a incidência dessa natureza é rara. Mas caso ocorra um fato desse existem sim penalidades para serem aplicadas
25) Há controle / Monitoramento de acesso físico aos servidores e equipamentos de rede.	1. Existe política descrita para acesso físico aos equipamentos em questão? 2. O acesso é monitorado? Como? 3. Quem autoriza e como?	Sim. Nenhum equipamento da empresa é acessado sem a supervisão e acompanhamento da TI. A TI da empresa autoriza previamente e faz todo o acompanhamento no local.
26) O controle de acesso ao CPD/Sala dos servidores e ativos é restringida fisicamente e monitorada por dispositivos autômatos	1. O acesso físico a sala dos equipamentos, servidores e ativos de rede é restringida por dispositivo de tranca? (Bio-métrico, dialpad, somente chave, etc)? O acesso é monitorado por câmeras e/ou outros dispositivos? Quais? 3. O Acesso é acompanhado por responsável designado? 2. O acesso a terceiros (prestadores de serviço e afins), é permitido? Como?	O acesso físico aos equipamentos de rede e servidores ficam dentro de um rack trancado por chave. E sim é monitorado por câmeras. Todo e qualquer acesso ao Rack é feito com o funcionário de TI.
27) Há sistemas de monitoramento de servidores e serviços	1. Existem sistemas de monitoramento dos servidores e serviços? Qual? 2. Os sistemas emitem alertas de problemas e/ou ameaças? Por quais meios? 3. Quais os tipos de monitoramento são aplicados? (Aplicação, serviços, invasões, etc)? 4. O acesso a tais sistemas é controlado? Como e por quem? Existe evidência?	Existem sim câmeras CFTV. Todo e qualquer acesso aos sistemas são registrados em log dentro do próprio aparelho de CFTV. O acesso é feito pelo TI.

28) Sistemas de segurança física para o ambiente de TI	1. Existem sistemas de monitoramento físico como CFTV, Alarmes e outros no TI? Quais? 2. Os acessos aos sistemas são monitorados? Como e por quem? Existe evidências? 3. No caso de CFTV, qual o período de retenção das imagens? Existe backup / redundância? 4. Os sistemas estão documentados? Favor evidenciar.	Existem sim câmeras CFTV. Todo e qualquer acesso aos sistemas são registrados em log dentro do próprio aparelho de CFTV. O acesso é feito pelo TI.
Requisitos Operacionais		
29) Acredita ter número suficiente de funcionários sugeridos para atendimento da conta no geral (atendimento e gestão)? Qual a função e a experiência de cada um?		Emissores Nacionais e Internacionais, Gerentes Operacionais, Equipe de Faturamento Todos com experiência superior a 2 anos.
30) Acredita ter o número de consultores sugeridos para atendimento? Qual a quantidade sugerida para atendimento? Tem capacidade hoje de disponibilizar funcionários para atendimento exclusivo, ou seja, sem atender nenhum outro cliente?		Sim, temos consultores escalonáveis a depender da quantidade de emissões. E se por ventura houver a necessidade de colocar exclusivo temos também.
31) Possui consultores especializados em rotas internacionais capazes de efetuar um planejamento da viagem e oferecer alternativas eficientes de rotas? Se sim, quantos? Quantos anos de experiência?		Sim, temos 3 consultores que preenchem os referidos requisitos com vasta experiência no mercado.
32) Possui consultores especializados em reservas/logística de hotéis e serviços internacionais? Se sim, quantos? Quantos anos de experiência?		Sim, temos 3 consultores que preenchem os referidos requisitos com vasta experiência no mercado.
33) Possui consultor bilíngue/ poliglota? Se sim, quantos?		Sim Bilingue. Temos 2 consultores.
34) Com quais fornecedores a agência atua com relação a seguro viagem? Tem experiência em contratação de seguro para algum esporte olímpico?		Travelace, Assist Card, Affinity. Sim. A agência já tem uma vasta experiência com o CPB e confederações esportivas.
35) Possui acordos com companhias aéreas nacionais e internacionais net? Os descontos podem ser compartilhado com o CBTArco		Sim temos.
36) Pode disponibilizar IATA dedicado A CBTArco para controle de acordos e volumes emitidos?		Sim Podemos
37) Quais as formas de pagamentos trabalhadas hoje na agência para hospedagem?		Faturamento e cartão de crédito
38) Trabalha com alguma operadora e/ou consolidadora?		Sim.

39) Possui consultor ou departamento especializado em atendimento a passageiros VIPs? O que está incluso no atendimento VIP?	Não.
40) Possui disponibilidade de oferecer consultores especializados na sede do CBTARCO para prestação de serviços? Em quanto tempo?	Sim. Disponibilizamos em 30 Dias
41) Em caso de necessidade de substituição de consultores ou funcionários, qual o tempo para substituição e treinamento? Tem essa disponibilidade?	Sim 30 dias
42) Possui alguma metodologia de avaliação dos consultores e atendimento prestado?	Sim.
43) Possui treinamentos e capacitações regulares com seus funcionários? Qual o tipo e frequência?	Sim a cada 60 dias ou conforme necessidade. Treinamentos diversos junto ao RH terceirizado
44) Possui algum tipo de controle interno de SLA? Quais?	Sim. Todos nossos sistemas possuem um tempo de resposta em caso de queda ou danos ao sistema. Temos tanto renúncia quanto máquinas prontas para imersão imediatamente em pane. Nossos consultores também trabalham com tempo de resposta satisfatório e prestamos um SLA no atendimento.
45) Possui gerente de contas (Key Account Manager)? Qual suas funções na agência? Qual a frequência de visitas para acompanhamento por mês?	Sim Gerente Comercial - as visitas são feitas semanalmente para os clientes locais e de 3 em 3 meses nos clientes fora do Estado ou conforme necessidade
46) Possui serviço de apoio, nos aeroportos das principais capitais, especialmente RIO, SP, BSB ? Próprio ou terceirizado?	Sim, Terceirizado
47) Os consultores fornecem recomendações para obtenção de vistos, passaportes, vacinas, etc.? É um serviço ativo, onde o viajante é informado dos documentos necessários quando ele faz a solicitação, ou o viajante terá que perguntar?	Nossos consultores são treinados e qualificados para toda e qualquer explicação e informação sobre documentos necessários para embarque e voos.

Recife, 05 de Fevereiro de 2021

Taciana Fernandes
DAHER TURISMO LTDA.
Taciana S. M. Fernandes
Diretora

