TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

Este questionário tem acesso controlado. É necessário um código de acesso válido para participar.
Se você recebeu um código de acesso, por favor digite-o na caixa abaixo e clique em Continuar.

Código de acesso:

Continuar

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

À medida que avançam as tecnologias da informação (TI), os processos de negócio das organizações dependem cada vez mais de bases de dados e de sistemas de informação. Assim, manter controles internos efetivos sobre os procedimentos de *backup* e *restore* tornou-se fundamental para assegurar a continuidade do negócio e a consequente prestação dos respectivos serviços públicos por parte dos órgãos e entidades da Administração Pública Federal (APF).

O Tribunal de Contas da União (TCU), por meio da presente auditoria, busca avaliar em que medida as organizações da APF realizam procedimentos de *backup* e *restore* de suas bases de dados e de seus sistemas.

O método utilizado é o de autoavaliação de controles internos (do inglês *Control Self Assessment* – CSA), no qual disponibiliza-se um questionário para que o gestor preencha as respostas que melhor reflitam a situação atual da sua organização com relação aos procedimentos de *backup* e *restore*. Além de fornecer ao órgão/entidade um diagnóstico do seu grau de maturidade atual com relação aos procedimentos questionados, essa metodologia permite que os gestores e a unidade de auditoria interna continuem avaliando a organização mesmo após o término da auditoria e, assim, conduzam, por conta própria, seu aumento de maturidade ao longo dos próximos anos, com a implantação dos controles internos necessários.

A fim de nortear o gestor respondente, esclarece-se que os critérios utilizados para subsidiar a elaboração do questionário foram livremente adaptados a partir do julgamento profissional da equipe de auditores do TCU sobre o controle nº 10 (*Data Recovery Capabilities*) da versão 7 do *framework* desenvolvido pelo Center for Internet Security (CIS).

Observações importantes:

1) O texto do questionário foi previamente validado com o intuito de evitar que o respondente tenha dúvidas quanto à melhor interpretação das perguntas e possibilidades de resposta correspondentes. Aconselha-se que o questionário seja preenchido assim que recebido, frisando-se que eventuais solicitações de esclarecimentos (a serem encaminhadas para o e-mail auditoria.backup@tcu.gov.br) podem não ser respondidas a tempo e que isso não justifica o não preenchimento completo e envio do questionário até 6/11/2020.

2) Por poderem conter informações sensíveis, as evidências (*upload* de arquivos) enviadas no âmbito desta auditoria serão, de antemão, classificadas como reservadas, nos termos do art. 23, inciso I, c/c art. 24, § 1º, inciso III, da Lei 12.527/2011 (Lei de Acesso à Informação – LAI).

3) Com esta auditoria, o TCU visa a diagnosticar a maturidade dos órgãos e entidades da APF em relação aos critérios questionados, ciente de que uma maturidade maior implica em custos mais elevados e que, portanto, a definição do grau de maturidade mais adequado a cada organização é, essencialmente, uma decisão de gestão (tomada com base no tipo de negócio, apetite a riscos, custo e expectativa de retorno da implementação de controles internos específicos etc.).

4) O respondente pode navegar à vontade entre os grupos de questões por meio dos botões "Próximo" e "Anterior" localizados no rodapé das páginas. O botão "Próximo", no entanto, só permitirá o avanço se as perguntas obrigatórias do grupo/página (marcadas com um asterisco vermelho) estiverem preenchidas. No ponto onde estiver, o respondente também pode clicar em "Retomar mais tarde" para salvar as respostas marcadas até então e voltar a preencher o questionário em outro momento. Após clicar em "Próximo" no último grupo de questões, haverá uma última tela com o intuito de garantir que o envio do questionário não seja feito até que o respondente tenha anexado todas as evidências solicitadas.

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

De acordo com Ofício de Comunicação enviado pelo TCU, cada organização deverá indicar um gestor para responder este questionário

Devido ao tema, sugere-se que o gestor respondente seja da área de tecnologia da informação (TI).

Este questionário envolve a solicitação de informações e o *upload* de evidências (documentos) que suportem as respostas fornecidas.

O preenchimento desta guia (identificação do respondente) deve ser feito **imediatamente**. O prazo final para o preenchimento das demais questões, *upload* das evidências e envio do questionário é 6/11/2020 (sexta-feira), até às 23h59.

Além de registrar o responsável por responder o questionário, a coleta desses dados ocorre para que a equipe de auditoria do TCU, se necessário, possa entrar em contato com o respondente para dirimir eventuais dúvidas.

* **Identificação do servidor indicado para responder o questionário:**

Nome completo do respondente:	
CPF do respondente:	
Cargo do respondente:	
Telefone (com DDD) do respondente:	
E-mail do respondente:	

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

PORTE DA ORGANIZAÇÃO E POLÍTICA DE BACKUP

O propósito dessas primeiras perguntas é permitir que, para fins de análise, a equipe de auditoria possa estratificar as organizações avaliadas de acordo com o respectivo porte e a existência ou não de política de *backup*.

Não se preocupe em fornecer os números exatos. Tampouco se espera que o respondente, caso não possua essas informações no momento, pare de responder o questionário até obtê-las.

Por favor, **informe agora** os números que mais se aproximam da realidade da sua organização, de acordo com o melhor do seu conhecimento. Se for o caso, é possível retornar depois (botão "Anterior" localizado no rodapé da página) para alterar qualquer um dos números fornecidos.

* **Qual é a quantidade total de colaboradores da organização?**

Pergunta obrigatória.

Apenas números podem ser usados nesse campo.

Por "colaborador", entende-se qualquer pessoa que trabalha para a organização (mesmo que remotamente), incluindo servidores/funcionários próprios, terceirizados, estagiários etc.

* **Quantos desses colaboradores atuam no setor de TI da organização?**

Pergunta obrigatória.

Apenas números podem ser usados nesse campo.

Por "atuar no setor de TI", entende-se que a atividade do colaborador está relacionada aos processos de trabalho e metas do setor de TI da organização.

* **A organização possui política de *backup* (ou instrumento normativo equivalente) documentada e aprovada formalmente?**

Escolha uma das seguintes respostas:

Pergunta obrigatória.

- ○ NÃO
- ○ SIM, existe política de backup documentada, porém ainda não aprovada formalmente
- ○ SIM, existe política de backup documentada e já aprovada formalmente

?

A política de *backup* é um acordo da área de TI com a área de negócio ("dona" dos dados e/ou sistemas), de caráter geral, no qual são documentados de quais dados (bases de dados, sistemas de arquivos, imagens de servidores etc.) serão feitos os *backups*, bem como as respectivas periodicidades (diária, semanal, mensal etc.), tipos (completo, diferencial ou incremental), quantidades de cópias, locais de armazenamento, tempos de retenção das cópias e requisitos específicos de segurança em função dos dados copiados (controle de acesso, localização remota, criptografia etc.). Esses requisitos podem variar de acordo com cada base de dados ou sistema da organização e, para as bases de dados/arquivos/sistemas/aplicativos/servidores mais críticos, esses requisitos podem, ainda, ser detalhados em documentos específicos, chamados planos (ou procedimentos/roteiros) de *backup*.

Anexe a política de *backup* (ou instrumento normativo equivalente) da organização:

Arquivos enviados

?

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 20 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for a própria política de *backup*, mas um documento mais abrangente que a contenha, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a política de *backup* (*e.g.* números das páginas, capítulo, seção, item, parágrafos etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco***.

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

Subcontrole 1: Realize cópias de segurança (backups) de todos os dados da organização, de forma regular e automática

Quando se fala em continuidade do negócio, a implementação deste subcontrole é crucial, pois permite que a organização se recupere de um ataque ou da disseminação de um *malware*, por exemplo, que possam comprometer seus dados, lembrando que, segundo dados da empresa Kaspersky, o Brasil "lidera a lista dos países mais afetados por ataques de *ransomware* empresariais ao redor do mundo" (https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527), sendo "alvo de quase metade dos ataques de *ransomware* na América Latina" (https://tiinside.com.br/15/10/2020/brasileiros-sao-alvo-de-quase-metade-dos-ataques-de-ransomware-na-america-latina).

Esclarece-se que esta auditoria irá avaliar a execução de cópias de segurança (*backups*) em relação à principal base de dados tratada diretamente pela organização.

* **1.1.** A organização trata diretamente alguma base de dados?

○ Sim ○ Não

? Por "diretamente", entende-se que a própria organização, e não algum órgão vinculador, é a principal responsável pela custódia e pelo tratamento dos referidos dados.

* **1.2.** Identifique a principal base de dados tratada diretamente pela organização:

* **1.3.** Qual é o tamanho aproximado, em MB, da principal base de dados tratada diretamente pela organização?

Apenas números podem ser usados nesse campo.

1.4. Indique, se houver, o(s) nome(s) da(s) ferramenta(s) utilizada(s) para gerenciar os *backups* da base de dados referida na pergunta 1.2:

* **1.5.** Em relação à base de dados referida na pergunta 1.2, com qual periodicidade são realizados *backups*:

	Completos (full)?	Diferenciais?	Incrementais?
Não são realizados	○	○	○
Mais de uma vez por dia	○	○	○
Diariamente	○	○	○
Semanalmente	○	○	○
Mensalmente	○	○	○
Ocasionalmente (menos do que uma vez por mês)	○	○	○

?

Completos (*full*): cópia integral da base de dados

Diferenciais: cópia dos registros alterados desde o último *backup full*

Incrementais: cópia dos registros alterados desde o último *backup*, seja ele *full* ou incremental

* **1.6.** Indique a forma de realização dos *backups* completos da base de dados referida na pergunta 1.2:

Escolha uma das seguintes respostas:

- ○ Manual
- ○ Automatizada
- ○ Outra forma

Por favor, coloque aqui o seu comentário:

Manual: algum funcionário precisa dar o comando para a execução do *backup*

Automatizada: o *backup* ocorre regularmente, de forma automática, de acordo com a periodicidade definida em ferramenta de gerenciamento

Outra forma: caso não se enquadre nas opções acima, descreva no campo de comentário

1.7. Anexe alguma evidência de que os *backups* completos da base de dados referida na pergunta 1.2 ocorrem de forma automatizada:

Arquivos enviados

Evidência sugerida: *print* da tela da ferramenta de gerenciamento de *backups* mostrando a configuração da periodicidade de realização dos *backups*.

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for uma simples imagem, como sugerido, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a evidência de que os *backups* completos ocorrem de forma automatizada (*e.g.* número da página, item, parágrafo, linha etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a produção da evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco***.

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

Subcontrole 2: Realize cópias de segurança (backups) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade

Há três tipos principais de *backup* (completo, incremental e diferencial), cada um com seus prós e contras, sobretudo no que se refere à rapidez com que os dados podem ser obtidos e restaurados.

Assim, uma organização com grau de maturidade mais elevado tende a definir e a manter um leque de *backups* de tipos variados, sempre levando em consideração as particularidades do seu negócio, o seu apetite a riscos, os custos associados e, principalmente, o *trade-off* ("perdas-e-ganhos") entre a performance na execução das cópias e a prontidão de sua eventual restauração, em caso de necessidade. Ela pode, por exemplo, executar um *backup* completo (*full*) semanalmente, com *backups* incrementais diários.

Relativamente a seus sistemas críticos, convém que a organização assegure que sejam realizados *backups* integrais (cópia/espelhamento da imagem dos servidores/máquinas envolvidos) periódicos, de modo que, em caso de necessidade, tais sistemas possam ser recuperados em curtíssimo espaço de tempo (a depender da criticidade do sistema, sua parada pode interromper/inviabilizar o negócio da organização como um todo).

Esclarece-se que esta auditoria irá avaliar a execução de cópias de segurança (*backups*) integrais em relação ao servidor ou conjunto de servidores/máquinas da própria organização que hospedam o principal sistema cuja gestão está sob sua responsabilidade.

* **2.1.** A organização hospeda, em servidor ou conjunto de servidores/máquinas próprios*, algum sistema cuja gestão está sob sua responsabilidade?

○ Sim ○ Não

?

*Esta pergunta não se refere a sistemas hospedados na "nuvem" (*cloud services*), pois a intenção do grupo de perguntas nesta tela é verificar a realização de cópias de segurança (*backups*) pela própria organização, não por empresa eventualmente contratada.

Por "gestão sob sua responsabilidade", entende-se que a própria organização, e não algum órgão vinculador, é a principal responsável pela manutenção, evolução e gerência do referido sistema.

* **2.2.** Identifique o principal sistema hospedado pela organização?

2.3. Indique, se houver, o(s) nome(s) da(s) ferramenta(s) utilizada(s) para gerenciar os *backups* do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2:

* **2.4.** Em relação ao servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2, com qual periodicidade são realizados os *backups*?

Escolha uma das seguintes respostas:

- ○ Não são realizados
- ○ Mais de uma vez por dia
- ○ Diariamente
- ○ Semanalmente
- ○ Mensalmente
- ○ Ocasionalmente (menos do que uma vez por mês)

* **2.5.** Indique a forma de realização dos *backups* do servidor ou conjunto de servidores/máquinas:
Escolha uma das seguintes respostas:

- ○ Parcial
- ○ Integral
- ○ Outra forma

Por favor, coloque aqui o seu comentário:

Parcial: cópia de determinados arquivos do(s) servidor(es)

Integral: cópia/espelhamento da imagem do(s) servidor(es) ou procedimento assemelhado

Outra forma: caso não se enquadre nas opções acima, descreva no campo de comentário

2.6. Anexe alguma evidência de que esses *backups* são integrais:

Arquivos enviados

Evidência sugerida: *print* de tela mostrando as propriedades do arquivo de *backup* integral mais recente do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2.

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for uma simples imagem, como sugerido, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a evidência de que os referidos *backups* são integrais (*e.g.* número da página, item, parágrafo, linha etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria.**

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a produção da evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco*.**

* **2.7.** A organização possui plano de *backup* específico para o sistema referido na pergunta 2.2?

○ Sim ○ Não

A política de *backup* é um acordo da área de TI com a área de negócio ("dona" dos dados e/ou sistemas), de caráter geral, no qual são documentados de quais dados (bases de dados, sistemas de arquivos, imagens de servidores etc.) serão feitos os *backups*, bem como as respectivas periodicidades (diária, semanal, mensal etc.), tipos (completo, diferencial ou incremental), quantidades de cópias, locais de armazenamento, tempos de retenção das cópias e requisitos específicos de segurança em função dos dados copiados (controle de acesso, localização remota, criptografia etc.). Esses requisitos podem variar de acordo com cada base de dados ou sistema da organização e, para as bases de dados/arquivos/sistemas/aplicativos/servidores mais críticos, esses requisitos podem, ainda, ser detalhados em documentos específicos, chamados planos (ou procedimentos/roteiros) de *backup*.

2.8. Anexe o plano de *backup* do sistema referido na pergunta 2.2:

Arquivos enviados

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 20 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for o próprio plano de *backup*, mas um documento mais abrangente que o contenha, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrado o plano de *backup* (*e.g.* números das páginas, capítulo, seção, item, parágrafos etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria.**

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco*.**

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

Subcontrole 3: Realize, periodicamente, testes de restauração (restore) das cópias de segurança (backups) da organização, de modo a atestar seu funcionamento em caso de necessidade

Além de garantir seu perfeito funcionamento em casos reais nos quais seja necessário restaurar algum *backup*, esses testes periódicos permitem que os gestores tenham maior clareza acerca dos custos associados à manutenção de controles efetivos de *backup/restore* e, com isso, percebam que implementar esses controles na organização, em geral, custa significativamente menos do que, em eventual caso de *ransomware* ("sequestro" de dados), acabar se vendo forçado a pagar o valor solicitado pelo criminoso cibernético a título de "resgate" dos dados (sob pena de parar o negócio da organização, por exemplo). Frisando-se que esse tipo de ataque cresceu 350% no Brasil desde janeiro de 2020 (https://olhardigital.com.br/coronavirus/noticia/ataques-de-ransomware-no-brasil-cresceram-3-5x-desde-janeiro-diz-kaspersky/98583).

Esclarece-se que esta auditoria irá avaliar a execução do procedimento de restauração (*restore*) em relação à base de dados referida na pergunta 1.2 (principal base de dados tratada diretamente pela organização) e ao servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2 (principal sistema hospedado pela organização).

* **3.1.** A organização executa, periodicamente, testes de restauração (*restore*) dos seus *backups*?

Escolha uma das seguintes respostas:

- ○ NÃO
- ○ SIM, mas somente em relação aos backups de sua principal base de dados
- ○ SIM, mas somente em relação aos backups dos servidores/máquinas que hospedam seu principal sistema
- ○ SIM, em relação a ambos backups, da principal base de dados e dos servidores/máquinas que hospedam seu principal sistema

?

Obs1.: Caso a resposta à pergunta 1.1 (A organização trata diretamente alguma base de dados?) tenha sido "Não", significa que a organização não realiza *backup* de nenhuma base de dados própria e, portanto, não faz sentido o respondente marcar aqui nenhuma das respostas afirmativas em relação a *restore* de *backup* de base de dados. Se isso ocorrer, será considerada marcada, para todos os efeitos, a resposta "NÃO".

Obs2.: Similarmente, caso a resposta à pergunta 2.1 (A organização hospeda, em servidor ou conjunto de servidores/máquinas próprios, algum sistema cuja gestão está sob sua responsabilidade?) tenha sido "Não", significa que a organização não realiza *backup* de nenhum servidor/máquina próprio/a e, portanto, não faz sentido o respondente marcar aqui nenhuma das respostas afirmativas em relação a *restore* de *backup* de servidores/máquinas. Se isso ocorrer, será considerada marcada, para todos os efeitos, a resposta "NÃO".

Obs3.: Consequentemente, caso tanto a resposta à pergunta 1.1 quanto a resposta à pergunta 2.1 tenham sido "Não" (significando que a organização não realiza *backup* de nenhuma base de dados ou servidor/máquina próprios), só faz sentido o respondente marcar aqui a resposta "NÃO" e, para todos os efeitos, essa será considerada a resposta marcada.

* **3.2.** Os testes de restauração (*restore*) são documentados (isto é, geram algum tipo de registro formal ou relatório de resultados)?

○ Sim ○ Não

3.3. Anexe o relatório de resultados (ou outro tipo de registro formal) do teste de *restore* mais antigo de 2020 (ou seja, relativo ao primeiro teste realizado este ano):

Arquivos enviados

?

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for o próprio relatório de resultados do *restore*, mas um documento mais abrangente que o contenha, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrado o referido relatório de resultados do *restore* (*e.g.* números das páginas, capítulo, seção, item, parágrafos etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco***.

* **3.4.** Com qual periodicidade são realizados os testes de restauração (*restore*) dos *backups*:

	Da base de dados referida na pergunta 1.2*?	**Do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2**?**
Não são realizados	○	○
Diariamente	○	○
Semanalmente	○	○
Mensalmente	○	○
A cada três meses	○	○
Ocasionalmente (menos do que uma vez a cada três meses)	○	○

?

*Principal base de dados tratada diretamente pela organização. Caso não se lembre qual é essa base de dados, o respondente pode retornar clicando no botão "Anterior" localizado no rodapé da página para conferir a resposta fornecida na pergunta 1.2.

**Principal sistema hospedado pela organização. Caso não se lembre qual é esse sistema, o respondente pode retornar clicando no botão "Anterior" localizado no rodapé da página para conferir a resposta fornecida na pergunta 2.2.

Obs1.: Caso a resposta à pergunta 1.1 (A organização trata diretamente alguma base de dados?) tenha sido "Não", a resposta quanto à periodicidade do *restore* da base de dados (1ª coluna) deve ser "Não são realizados".

Obs2.: Caso a resposta à pergunta 2.1 (A organização hospeda, em servidor ou conjunto de servidores/máquinas próprios, algum sistema cuja gestão está sob sua responsabilidade?) tenha sido "Não", a resposta quanto à periodicidade do *restore* do servidor/conjunto de servidores (2ª coluna) deve ser "Não são realizados".

3.5. Anexe alguma evidência da realização do teste de restauração (*restore*) mais recente de *backup* da base de dados referida na pergunta 1.2 (principal base de dados tratada diretamente pela organização):

Arquivos enviados

Evidência sugerida: *print(s)* de tela da ferramenta de gerenciamento de *backups* mostrando que o procedimento de *restore* foi realizado com sucesso.

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for uma simples imagem, como sugerido, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a evidência da realização do *restore* (*e.g.* número da página, item, parágrafo, linha etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a produção da evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco***.

3.6. Anexe alguma evidência da realização do teste de restauração (*restore*) mais recente de *backup* do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2 (principal sistema hospedado pela organização):

Arquivos enviados

Evidência sugerida: *print(s)* de tela da ferramenta de gerenciamento de *backups* mostrando que o procedimento de *restore* foi realizado com sucesso.

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for uma simples imagem, como sugerido, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a evidência da realização do *restore* (*e.g.* número da página, item, parágrafo, linha etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a produção da evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco***.

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

Subcontrole 4: Proteja adequadamente as cópias de segurança (backups) da organização, por meio de mecanismos de controle de acesso físico e lógico

Uma vez que, nos casos de *ransomware*, os profissionais de segurança das organizações com grau de maturidade mais elevado passaram a realizar procedimentos de restauração (*restore*) de *backups* ao invés de pagarem os valores solicitados a título de "resgate" dos dados, os criminosos cibernéticos e seus *malwares*, progressivamente, passaram a incluir os próprios arquivos de *backup* entre os alvos principais dos ataques.

Com isso, torna-se cada vez mais importante a implementação de mecanismos de controle de acesso físico (*e.g.* ambiente segregado) e lógico (*e.g.* criptografia) relativamente aos arquivos de cópias de segurança (*backups*). Ademais, visto que muitos *backups* são armazenados em sítios remotos ou mesmo em servidores hospedados na "nuvem" (*cloud services*), faz-se necessário implementar controles criptográficos não apenas quanto aos arquivos armazenados (*data at rest*), mas, também, quanto aos arquivos que trafegam na rede da organização ou na Internet (*data in transit*).

Esclarece-se que esta auditoria irá avaliar os mecanismos de controle de acesso físico e lógico existentes em relação aos arquivos das cópias de segurança (*backups*) que o respondente, no contexto da sua organização, considerar que são os mais bem protegidos entre aqueles referidos nas questões anteriores (arquivos de *backup* da principal base de dados tratada pela organização e do servidor ou conjunto de servidores/máquinas que hospedam o principal sistema da organização).

* **4.1.** Os arquivos dos *backups* da organização* são armazenados:
Escolha uma das seguintes respostas:

- ○ A organização não realiza backups
- ○ Somente na própria sede da organização
- ○ Somente em um sítio remoto sob gestão da própria organização
- ○ Somente em um servidor hospedado na "nuvem"**
- ○ Na própria sede da organização, com cópia/espelhamento em outra localidade sob gestão da organização
- ○ Na própria sede da organização, com cópia/espelhamento em um servidor hospedado na "nuvem"**
- ◉ Na própria sede da organização, com cópia/espelhamento em outra localidade sob gestão da organização E em um servidor hospedado na "nuvem"**

?

*Responder em relação aos *backups* que o respondente, no contexto da sua organização, considerar que são os mais bem protegidos entre aqueles referidos nas questões anteriores (arquivos de *backup* da principal base de dados tratada pela organização e do servidor ou conjunto de servidores/máquinas que hospedam o principal sistema da organização).

**Contratação de serviços de hospedagem na "nuvem" (*cloud services*).

4.2. Indique o endereço da localidade remota onde são armazenados os *backups*:

* **4.3.** No caso de contratação de serviços de hospedagem na "nuvem" (*cloud services*), qual(is) é(são) a(s) empresa(s) contratada(s)?
Escolha a(s) que mais se adeque(m)

- ☐ Alibaba
- ☐ Amazon
- ☐ AT&T
- ☐ Dataprev
- ☐ Google
- ☐ HP
- ☐ IBM
- ☐ Microsoft
- ☐ Serpro
- ☐ Outra(s) empresa(s)*

? *Outra(s) empresa(s): caso não esteja(m) relacionada(s), escreva o(s) nome(s) da(s) empresa(s) no campo de comentário

* **4.4.** No local de armazenamento*, os arquivos dos *backups*:
Escolha uma das seguintes respostas:

- ○ Não são armazenados criptografados
- ○ Recebem apenas criptografia de armazenamento**
- ○ Recebem a chamada "criptografia de ponta-a-ponta"***

?

*Caso haja armazenamento tanto sob gestão da própria organização quanto na "nuvem" (*cloud services*), favor responder em relação ao local que o respondente considera ser o mais seguro.

**Criptografia de armazenamento: o processo de criptografia/descriptografia ocorre somente no servidor de *backup* ou no servidor do provedor de "nuvem" e, portanto, o arquivo trafega em claro na rede da organização ou na Internet.

***Criptografia de ponta-a-ponta: o processo de criptografia/descriptografia ocorre em aplicativo na estação do cliente e, portanto, o arquivo não trafega em claro na rede da organização ou na Internet.

* **4.5.** O local de armazenamento dos arquivos dos *backups*, **sob gestão da própria organização***, considerado o mais seguro pelo respondente:
Escolha uma das seguintes respostas:

- ○ Não possui mecanismo de controle de acesso físico
- ○ É um ambiente segregado, com mecanismo de controle de acesso físico apenas mecânico**
- ○ É um ambiente segregado, com mecanismo de controle de acesso físico que inclui dispositivo eletrônico***

?

*Favor responder considerando somente o local de armazenamento sob gestão da própria organização (NÃO RESPONDER em relação a eventual hospedagem na "nuvem").

***E.g.* porta com chave.

****E.g.* porta com fechadura eletrônica.

* **4.6.** A permissão de acesso ao ambiente segregado em questão é concedida a partir de algo que somente o usuário:
Escolha uma das seguintes respostas:

- ○ Sabe
- ○ Possui
- ○ É
- ○ Combinação dos fatores anteriores

?

Sabe: *e.g.* abertura por senha

Possui: *e.g.* abertura por chave física ou cartão de acesso

É: *e.g.* abertura a partir de característica biométrica (impressão digital, íris etc.)

Combinação: *e.g.* cartão de acesso e senha, impressão digital e senha

4.7. Anexe alguma evidência da existência do mecanismo de controle de acesso físico em questão:

Arquivos enviados

?

Evidência sugerida: fotografia(s) da porta do ambiente segregado, mostrando o mecanismo de controle de acesso físico.

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for uma simples imagem, como sugerido, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a evidência da existência do mecanismo de controle de acesso físico em questão (*e.g.* número da página, item, parágrafo, linha etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a produção da evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco***.

* **4.8.** Os acessos ao ambiente segregado são registrados (isto é, há *log* desses acessos, contendo identificador, data/hora e nome da pessoa que acessou)?

○ Sim ○ Não

4.9. Anexe alguma evidência de que os acessos ao ambiente segregado são registrados:

Arquivos enviados

Evidência sugerida: fotografia da folha de registro (se o procedimento for manual) ou *print(s)* de tela do arquivo de *log* mostrando os dados registrados (identificador, data/hora, nome da pessoa que acessou etc.).

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for o próprio registro dos acessos ao ambiente, mas um documento mais abrangente que os contenha, por favor descreva nesse campo o local exato, no arquivo/documento, onde podem ser encontrados os referidos registros dos acessos ao ambiente (*e.g.* números das páginas, capítulo, seção, item, parágrafos etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria.**

Obs3.: Para possibilitar o avanço no preenchimento do questionário enquanto se providencia a evidência solicitada, esta questão foi configurada como opcional. Contudo, se avançar (clicar em "Próximo" no rodapé da página) sem realizar o *upload* do arquivo com a evidência, o respondente deve lembrar de retornar depois e realizar esse *upload*. **A organização que não efetuar o *upload* de alguma das evidências solicitadas poderá ser selecionada para auditoria *in loco*.**

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

Subcontrole 5: Armazene as cópias de segurança (backups) da organização em ao menos um destino não acessível remotamente

Uma vez que a programação dos *malwares* começou a incluir os próprios arquivos de *backup* entre os alvos dos ataques, fez-se necessário garantir que ao menos uma cópia desses arquivos fosse armazenada e mantida de modo *off-line*, isto é, não acessível pela rede da organização, seja por meio de chamadas de sistema operacional, de chamadas de API (*Application Programming Interface*) ou por qualquer outro meio de acesso remoto.

Idealmente, esse armazenamento é realizado em fitas próprias para *backup* (*e.g.* fita LTO) ou em discos rígidos (HDs), mas organizações menores/de menor maturidade podem fazer uso de DVDs, de CDs ou até de *pendrives*. Nesse último caso, porém, há risco maior de vazamento de dados ou de comprometimento dos arquivos, tendo em vista que esses dispositivos podem ser mais facilmente transportados, extraviados e/ou acoplados em estações de trabalho ou *notebooks* conectados à rede, perdendo, assim, sua característica *off-line*.

Esclarece-se que esta auditoria irá avaliar este subcontrole em relação aos arquivos das cópias de segurança (*backups*) tanto da principal base de dados tratada pela organização quanto do servidor ou conjunto de servidores/máquinas que hospedam o principal sistema da organização.

* **5.1.** A organização mantém seus *backups** em ao menos um destino não acessível remotamente?

Escolha uma das seguintes respostas:

- ◯ NÃO
- ◯ SIM, mas somente em relação aos backups da sua principal base de dados
- ◯ SIM, mas somente em relação aos backups dos servidores/máquinas que hospedam seu principal sistema
- ◯ SIM, em relação a ambos backups, da principal base de dados e dos servidores/máquinas que hospedam seu principal sistema

?

*Responder em relação aos *backups* tanto da principal base de dados tratada pela organização quanto do servidor ou conjunto de servidores/máquinas que hospedam o principal sistema da organização.

Obs1.: Caso a resposta à pergunta 1.1 (A organização trata diretamente alguma base de dados?) tenha sido "Não", não devem ser marcadas aqui as respostas "SIM, mas somente em relação aos *backups* de bases de dados" nem "SIM, em relação a ambos *backups*, de bases de dados e de servidores/máquinas".

Obs2.: Caso a resposta à pergunta 2.1 (A organização hospeda, em servidor ou conjunto de servidores/máquinas próprios, algum sistema cuja gestão está sob sua responsabilidade?) tenha sido "Não", não devem ser marcadas aqui as respostas "SIM, mas somente em relação aos *backups* de servidores/máquinas" nem "SIM, em relação a ambos *backups*, de bases de dados e de servidores/máquinas".

Obs3.: Consequentemente, caso as respostas a ambas perguntas 1.1 e 2.1 tenham sido "Não", o respondente deve marcar aqui a resposta "NÃO".

* **5.2.** Em qual mídia não acessível remotamente são armazenados os *backups* da base de dados referida na pergunta 1.2 (principal base de dados tratada diretamente pela organização)?

Escolha uma das seguintes respostas:

- ○ Pendrive
- ○ CD/DVD
- ○ Disco rígido (HD)
- ○ Fita
- ○ Outra mídia

Por favor, coloque aqui o seu comentário:

? Outra mídia: caso não se enquadre nas opções acima, descreva no campo de comentário

* **5.3.** Em qual mídia não acessível remotamente são armazenados os *backups* do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2 (principal sistema hospedado pela organização)?

Escolha uma das seguintes respostas:

- ○ Pendrive
- ○ CD/DVD
- ○ Disco rígido (HD)
- ○ Fita
- ○ Outra mídia

Por favor, coloque aqui o seu comentário:

? Outra mídia: caso não se enquadre nas opções acima, descreva no campo de comentário

5.4. Anexe alguma evidência da existência da mídia não acessível remotamente em questão relativamente ao *backup* mais recente da base de dados referida na pergunta 1.2 (principal base de dados tratada diretamente pela organização):

Arquivos enviados

Evidência sugerida: fotografia(s) da mídia sendo acessada localmente e mostrando as propriedades do arquivo de *backup* mais recente.

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for uma simples imagem, como sugerido, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a evidência da existência da mídia em questão (*e.g.* número da página, item, parágrafo, linha etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Esta questão foi configurada como opcional. Contudo, se o respondente clicar em "Enviar" no rodapé da página sem realizar o *upload* do arquivo com esta ou qualquer das outras evidências solicitadas em questões anteriores, **a organização poderá ser selecionada para auditoria *in loco***.

5.5. Anexe alguma evidência da existência da mídia não acessível remotamente em questão relativamente ao *backup* mais recente do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2 (principal sistema hospedado pela organização):

Arquivos enviados

Evidência sugerida: fotografia(s) da mídia sendo acessada localmente e mostrando as propriedades do arquivo de *backup* mais recente.

Obs1.: Só é aceito o *upload* de um único arquivo, do tipo PDF, com tamanho máximo de 10 MB. Caso o arquivo original da evidência não seja do tipo PDF, salve-o em PDF antes de fazer o *upload*.

Obs2.: Ao clicar em "Arquivos enviados" para realizar o *upload* do arquivo, será aberto um campo de comentário. Se o arquivo a ser enviado não for uma simples imagem, como sugerido, por favor descreva nesse campo o local exato, no arquivo/documento, onde pode ser encontrada a evidência da existência da mídia em questão (*e.g.* número da página, item, parágrafo, linha etc.). **É importante que seja indicada a localização exata da evidência para assegurar que ela seja considerada pela equipe de auditoria**.

Obs3.: Esta questão foi configurada como opcional. Contudo, se o respondente clicar em "Enviar" no rodapé da página sem realizar o *upload* do arquivo com esta ou qualquer das outras evidências solicitadas em questões anteriores, **a organização poderá ser selecionada para auditoria *in loco***.

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

Avaliação pessoal do respondente sobre a aderência da organização em relação a cada um dos cinco subcontroles

A fim de viabilizar a evidenciação, as perguntas anteriores foram feitas em relação à principal base de dados da organização e aos servidores/máquinas que hospedam o principal sistema da organização.

No entanto, naturalmente, é sabido que a implementação desses controles deve ser feita em relação a **todos os dados e sistemas da organização**. A título de exemplo, tem-se repositórios de arquivos (documentos), caixas postais do(s) servidor(es) de correio eletrônico etc.

Dito isso, frisa-se que o objetivo da pergunta a seguir é **registrar a avaliação (percepção) pessoal do respondente** quanto ao grau de aderência da sua organização em relação aos cinco subcontroles, **quando considerados os dados e os sistemas da organização como um todo**.

O objetivo desse registro é realizar um diagnóstico geral que se aproxime o máximo possível da realidade atual da organização. Portanto, solicita-se que o respondente procure avaliar com sinceridade, evitando, sobretudo, superestimar qualquer resposta.

As respostas a essa pergunta servirão, sobretudo, para que a própria organização possa ter uma ideia mais clara da sua evolução, quando de nova aplicação deste questionário dentro de alguns anos.

* **6.1.** Em relação a cada um dos cinco subcontroles abaixo e **considerando os dados e os sistemas da organização como um todo**, numa escala de 1 (nenhuma aderência) a 10 (aderência total), qual seria a avaliação pessoal do respondente em relação à sua organização?

	1	2	3	4	5	6	7	8	9	10
Subcontrole 1: Realize cópias de segurança (backups) de todos os dados da organização, de forma regular e automática	○	○	○	○	○	○	○	○	○	○
Subcontrole 2: Realize cópias de segurança (backups) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade	○	○	○	○	○	○	○	○	○	○
Subcontrole 3: Realize, periodicamente, testes de restauração (restore) das cópias de segurança (backups) da organização, de modo a atestar seu funcionamento em caso de necessidade	○	○	○	○	○	○	○	○	○	○
Subcontrole 4: Proteja adequadamente as cópias de segurança (backups) da organização, por meio de mecanismos de controle de acesso físico e lógico	○	○	○	○	○	○	○	○	○	○
Subcontrole 5: Armazene as cópias de segurança (backups) da organização em ao menos um destino não acessível remotamente	○	○	○	○	○	○	○	○	○	○

6.2. Se julgar necessário, registre aqui os principais desafios, deficiências e pontos de atenção relacionados à execução dos procedimentos de *backup* e *restore* da organização, bem como quaisquer outras considerações ou comentários que considerar pertinentes:

TRIBUNAL DE CONTAS DA UNIÃO

Auditoria sobre backup

0% 100%

LEIA COM MUITA ATENÇÃO!!!

Esta tela existe apenas para garantir que o envio do questionário não seja feito até que o respondente tenha anexado todas as evidências solicitadas.

Ao atingir este ponto, o respondente já respondeu todas as questões da auditoria consideradas obrigatórias, mas pode ter deixado de anexar alguma das evidências solicitadas (**política de *backup* e questões 1.7, 2.6, 2.8, 3.3, 3.5, 3.6, 4.7, 4.9, 5.4 e 5.5**).

Essas questões foram propositalmente configuradas como opcionais, caso contrário o respondente ficaria impossibilitado de avançar no questionário enquanto não produzisse e anexasse cada evidência. No entanto, frisa-se que **a anexação das evidências não é opcional, sendo que a organização que deixar de fazê-lo em relação a alguma delas poderá ser selecionada para auditoria *in loco*.**

Por favor, clique sucessivas vezes no botão "Anterior" localizado no rodapé desta e das demais páginas e confira as respostas fornecidas nas questões de todos os cinco grupos/subcontroles, sobretudo se foram devidamente realizados os *uploads* de todos os arquivos de evidências nas questões mencionadas acima (política de *backup* e 1.7, 2.6, 2.8, 3.3, 3.5, 3.6, 4.7, 4.9, 5.4 e 5.5). Lembrando que, a depender das respostas fornecidas, algumas dessas questões podem não ter sido abertas no seu questionário.

Após essa verificação, retorne a esta tela clicando sucessivamente no botão "Próximo" e, somente então, clique no botão "Enviar" para finalizar o questionário e submeter as respostas para análise dos auditores do TCU.

Se todas as evidências ainda não tiverem sido providenciadas e carregadas, é possível clicar em "Retomar mais tarde" e voltar a preencher o questionário em outro momento.

OBS1.: APÓS CLICAR NA OPÇÃO "ENVIAR" ABAIXO, NÃO SERÁ POSSÍVEL REALIZAR AJUSTES NAS RESPOSTAS FORNECIDAS.

OBS2.: O PRAZO PARA SUBMISSÃO DO QUESTIONÁRIO É 6/11/2020 (SEXTA-FEIRA). SE, ATÉ ÀS 23H59 DESSA DATA, ALGUMA EVIDÊNCIA AINDA ESTIVER PENDENTE, É PREFERÍVEL ENVIAR O QUESTIONÁRIO COM A PENDÊNCIA DO QUE DEIXAR DE ENVIÁ-LO.

* O respondente confirma que leu e compreendeu os termos acima, verificou que todas as evidências já foram devidamente anexadas nas questões pertinentes e concorda em enviar definitivamente suas respostas (após o envio, não será mais possível realizar qualquer ajuste nas respostas)?

○ Sim ○ Não