

**Auditoria sobre a efetividade dos procedimentos
de *backup* das organizações públicas federais
(TC 036.620/2020-3)**

Relatório Individual de Autoavaliação

**TRE-RR
Tribunal Regional Eleitoral de Roraima**

	A classificação deste documento é de responsabilidade da organização. Entretanto, em atenção à Lei 12.527/2011 (Lei de Acesso à Informação – LAI), art. 3º, inciso I, e art. 6º, inciso I, <u>o TCU sugere que este relatório não seja classificado como sigiloso</u> e que, ao contrário, a organização o publique em seu sítio na Internet e lhe dê ampla divulgação.	
---	---	---

SUMÁRIO

1. Introdução	2
2. Respostas registradas.....	3
Identificação da organização e do respondente	3
Política de <i>backup</i>	4
Subcontrole 1: Realize cópias de segurança (<i>backups</i>) de todos os dados da organização, de forma regular e automática	5
Subcontrole 2: Realize cópias de segurança (<i>backups</i>) integrais dos sistemas críticos da organização, de forma regular e automática	7
Plano de <i>backup</i>	8
Subcontrole 3: Realize, periodicamente, testes de restauração (<i>restore</i>) das cópias de segurança (<i>backups</i>) da organização, de modo a atestar seu funcionamento em caso de necessidade	9
Subcontrole 4: Proteja adequadamente as cópias de segurança (<i>backups</i>) da organização, por meio de mecanismos de controle de acesso físico e lógico	10
Subcontrole 5: Armazene as cópias de segurança (<i>backups</i>) da organização em ao menos um destino não acessível remotamente	12
Avaliação pessoal do respondente sobre a aderência da organização em relação a cada um dos cinco subcontroles	13
3. Relatório Comparativo de <i>Feedback</i>	15
4. Perspectiva para o futuro	16
Anexo I - <i>Checklists</i> para verificação de política e plano de <i>backup</i>	17
Anexo II - Avaliação da política de <i>backup</i>	19
Anexo III - Avaliação do plano de <i>backup</i>	20

1. Introdução

A Secretaria de Fiscalização de Tecnologia da Informação (Sefti) finalizou, recentemente, levantamento abrangente sobre a governança e a gestão da segurança da informação e da segurança cibernética na Administração Pública Federal (APF), no âmbito do qual foi identificada a necessidade de se elevar a maturidade geral das organizações da APF nessas áreas.

Os diagnósticos resultantes dessa fiscalização levaram, então, à proposição de uma estratégia de atuação para que o Tribunal de Contas da União (TCU), ao longo dos próximos anos, acompanhe e induza a boa gestão dessas áreas nos órgãos e entidades da APF, bem como contribua para disseminar a cultura de segurança no Estado e na sociedade, com a consequente minimização dos riscos e dos possíveis impactos de incidentes de segurança da informação e de ataques cibernéticos (**Figura 1**).

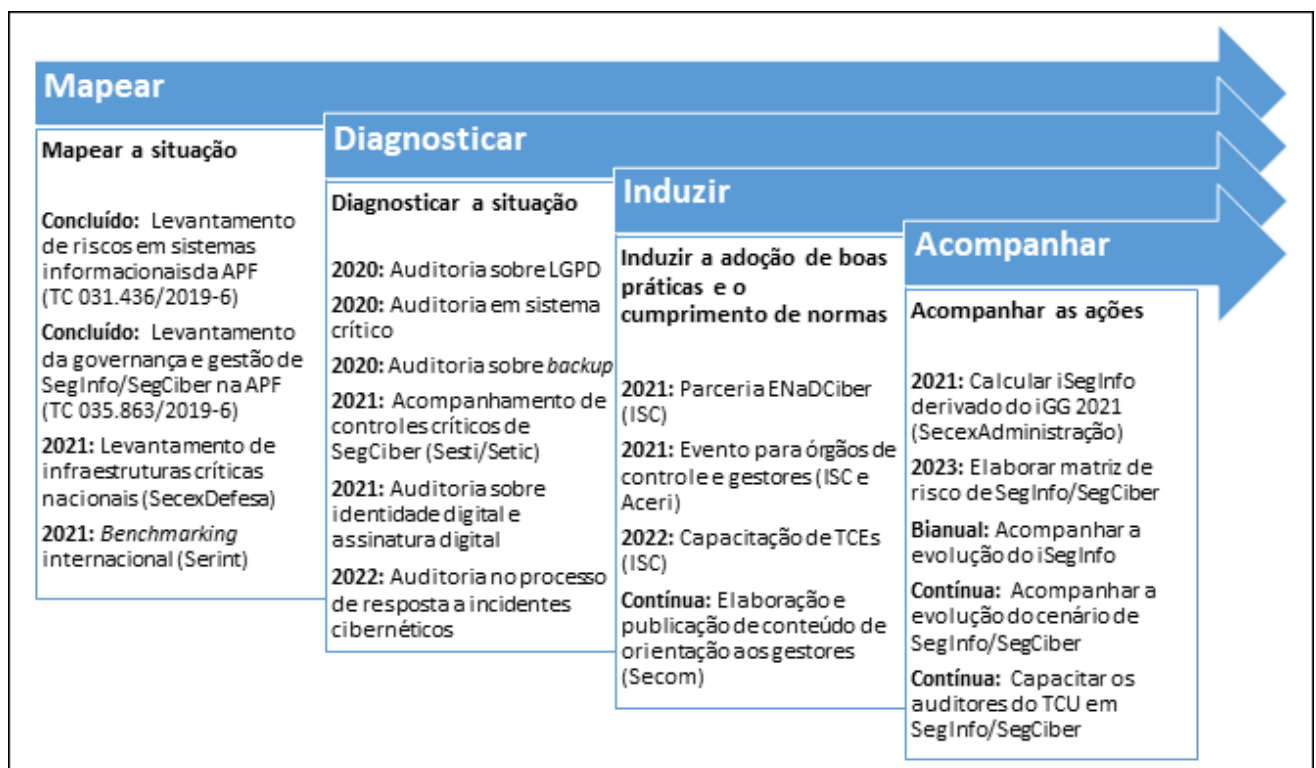


Figura 1 - Estratégia de atuação do TCU em segurança da informação e segurança cibernética.

(Fonte: elaboração própria)

Conferindo concretude à referida estratégia, a Sefti, em parceria com outras doze unidades técnicas da Secretaria-Geral de Controle Externo do TCU (SecexAdministração, SecexAgroAmbiental, SecexDefesa, SecexEducação, SecexEstataisRJ, SecexFinanças, SecexSaúde, SecexTrabalho, SeinfraPetróleo, SeinfraPortoFerrovia, SeinfraRodoviaAviação, SeinfraUrbana), coordenou a realização de auditoria específica com vistas a avaliar se os procedimentos de *backup* e *restore* dos órgãos e entidades da APF, mais especificamente sobre suas principais bases de dados e sistemas críticos, são suficientes e adequados para garantir a continuidade dos serviços prestados.

Este relatório apresenta as respostas individuais fornecidas por essa organização e, onde considerado oportuno, análises efetuadas pela equipe de auditores do Tribunal.

2. Respostas registradas

Identificação da organização e do respondente

Dados da organização	
Sigla:	TRE-RR
Nome:	Tribunal Regional Eleitoral de Roraima
Quantidade de colaboradores:	10
Quantidade de colaboradores que atuam no setor de TI:	4
Dados do servidor que respondeu o questionário	
Nome completo:	PAULO CEZAR RODRIGUES DA SILVA
CPF:	67794882591
Cargo:	Secretário de Tecnologia da Informação e Comunicação

Política de *backup*

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*.

Diante disso, a organização foi questionada quanto à existência de política de *backup* e, em caso afirmativo, o documento correspondente foi solicitado para análise.

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

NÃO

Para avaliar qualitativamente os documentos anexados pelos respondentes como sendo as políticas de *backup* das respectivas organizações, foi utilizado um *checklist* elaborado com base no item 12.3.1 (Cópias de segurança das informações) da norma ABNT NBR ISO/IEC 27002:2013, que especifica que “convém que cópias de segurança [*backups*] das informações, dos *software* e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida” (Anexo I).

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 a auditoria avaliou a execução de cópias de segurança (*backups*) apenas em relação à principal base de dados tratada diretamente pela organização.

1.1. A organização trata diretamente alguma base de dados?

Sim

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

Banco de dados dos sistemas administrativos

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

205107

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:

Oracle RMAN

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

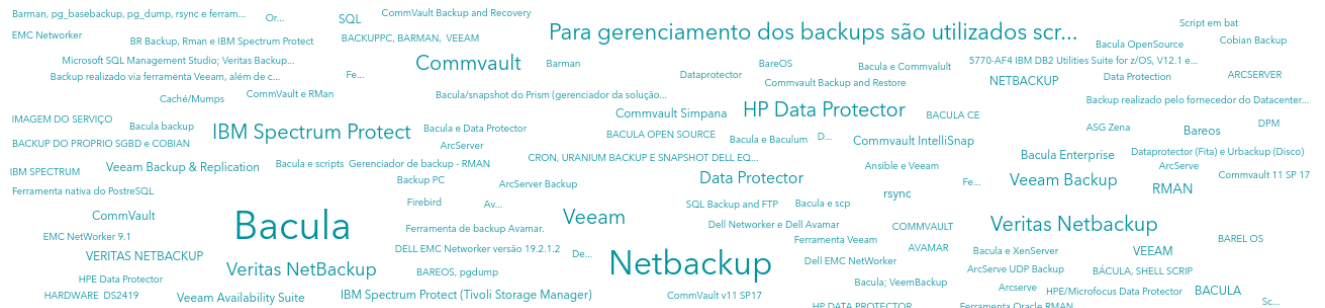
Completos (full)?	Diariamente
Diferenciais?	Não são realizados
Incrementais?	Não são realizados

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

Automatizada. O Oracle RMAN, utilitário da Oracle foi configurado para ser executado de forma automática 02 vezes ao dia.

1.7. Solicitação de evidência.

A seguir, encontra-se uma nuvem na qual o tamanho das palavras ou expressões é proporcional ao número de vezes que essas foram citadas por todas as organizações auditadas nas respostas à pergunta 1.4.



Embora o TRE-RR tenha afirmado que procede a realização de *backups*, de forma automatizada, não acostou a evidência, podendo o referido órgão ser, portanto, incluído em futura fiscalização *in loco*.

Subcontrole 2: Realize cópias de segurança (*backups*) integrais dos sistemas críticos da organização, de forma regular e automática

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 o desempenho 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 a auditoria avaliou a execução de cópias de segurança (*backups*) integrais apenas 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?

Não

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* dos 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*:

2.5. Indique a forma de realização dos *backups* do servidor ou conjunto de servidores/máquinas:

2.6. Solicitação de evidência.

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

N/A

Sugere-se que a organização procure se estruturar para realizar os *backups* do(s) referido(s) servidor(es) ao menos semanalmente, tendo em vista que uma periodicidade superior a essa (realização menos frequente do que uma vez por semana) pode ocasionar impacto significativo no negócio em caso de materialização de algum problema que implique necessidade de recuperação/restauração do *backup*.

Sugere-se, ainda, que a organização procure se estruturar para realizar, regularmente, cópias de segurança (*backups*) integrais de seus servidores/máquinas, sobretudo daqueles que hospedam os sistemas críticos. Esse tipo de cópia também é chamado de “imagem” e, em essência, consiste no espelhamento (cópia “bit a bit”) do(s) servidor(es) ou procedimento assemelhado, de modo que, em caso de necessidade, seja possível restaurar rapidamente o sistema a um estado anterior “estável”.

Plano de *backup*

Para avaliar qualitativamente o documento anexado pelo respondente como sendo o plano de *backup* do sistema referido na pergunta 2.2, também foi utilizado um *checklist* elaborado com base no item 12.3.1 (Cópias de segurança das informações) da norma ABNT NBR ISO/IEC 27002:2013 (Anexo I).

O Anexo III contém a avaliação do referido plano de *backup*.

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 a auditoria avaliou a execução do procedimento de restauração (*restore*) apenas 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*?

SIM, mas somente em relação aos backups de sua principal base de dados

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

Não

3.3. Solicitação de evidência.

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

Da base de dados referida na pergunta 1.2?	Ocasionalmente (menos do que uma vez a cada três meses)
Dos servidores/máquinas que hospedam o sistema referido na pergunta 2.2?	Não são realizados

3.5. Solicitação de evidência.

3.6. Solicitação de evidência.

Sugere-se que a organização procure se estruturar para realizar os testes de restauração (*restore*) dos *backups* ao menos mensalmente, tendo em vista que uma periodicidade superior a essa (realização menos frequente do que uma vez por mês) aumenta o risco para a organização.

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 a auditoria avaliou 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, considerou serem 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?

Somente na própria sede da organização

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)?

N/A

4.4. No local de armazenamento, os arquivos dos *backups*:

Não são armazenados criptografados

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

É um ambiente segregado, com mecanismo de controle de acesso físico apenas mecânico**

4.6. A permissão de acesso ao ambiente segregado em questão é concedida a partir de algo que somente o usuário:

Possui

4.7. Solicitação de evidência.

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)?

Não

4.9. Solicitação de evidência.

Sugere-se que a organização procure se estruturar para realizar o armazenamento e, idealmente, também o tráfego dos seus arquivos de *backup* pela rede e/ou Internet sempre criptografados, pois esse controle mitiga o risco de vazamento de dados.

Sugere-se, ainda, a instalação de dispositivo eletrônico na entrada do ambiente segregado em questão, pois, em relação a mecanismos meramente mecânicos, o primeiro permite implementar uma série de controles adicionais (e.g. permissão de acesso condicional ao dia da semana/horário, permissão de acesso baseada em perfis ou em características biométricas dos usuários etc.), além de possibilitar a geração e a guarda automatizada de *logs* (registros contendo informações relativas a cada acesso ao ambiente, a exemplo de um identificador, da data/hora de entrada/saída e da identificação do usuário).

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 a auditoria avaliou 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?

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)?

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)?

5.4. Solicitação de evidência.

5.5. Solicitação de evidência.

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

O respondente foi instado a avaliar o grau de aderência da organização em relação a cada um dos cinco subcontroles mencionados anteriormente, considerando os dados e os sistemas da organização como um todo (e não apenas em relação à principal base de dados e/ou ao principal sistema).

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?

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

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:

Desafios: Implementação de solução de armazenamento independente e com dados criptografados, atendendo aos requisitos orçamentários.

Deficiência: Planejamento para aquisições eficientes que atendam aos requisitos de segurança da informação o qual já está sendo tratado.

O respondente enfatiza que o TRE-RR evidencia como desafio a implementação de solução de armazenamento independente e com dados criptografados, bem como o desafio no planejamento para aquisições eficientes.

Além disso, o respondente reconheceu as deficiências da organização quanto apenas aos subcontroles 3, 4 e 5.

No entanto, entende-se que houve uma incongruência em relação aos Subcontroles 2 e 4, uma vez que o TRE-RR não realiza backup integral, ou parcial, de seus servidores/máquinas, e nem possui plano de *backup*. bem como não realiza testes periódicos de restauração e não possui instalado um dispositivo eletrônico na entrada do ambiente

segregado, nem tampouco implementou o registro de controle de acesso ao ambiente segregado.

As respectivas seções deste relatório contêm algumas orientações para que a organização aumente seu nível de maturidade em relação a esses subcontroles.

3. Relatório Comparativo de *Feedback*

Além deste “Relatório Individual de Autoavaliação”, a organização poderá receber um ou mais “Relatórios Comparativos de *Feedback*”, a fim de que possa comparar suas respostas individuais com aquelas de um ou mais conjuntos de organizações similares.

Esses relatórios comparativos especificarão, logo no início, todas as organizações que fazem parte do referido “conjunto” e, em essência, trarão a distribuição das respostas fornecidas por todas essas organizações em cada uma das respostas do questionário.

Com isso, espera-se que as organizações que demonstraram menor maturidade em relação aos subcontroles questionados no âmbito desta auditoria (conforme respostas fornecidas às diferentes perguntas do questionário) sintam-se incentivadas a evoluir ao longo dos próximos anos.

4. Perspectiva para o futuro

Ao longo dos próximos anos, a organização pode esperar auditorias relativas aos demais controles de segurança cibernética do *framework* do *Center for Internet Security* – CIS (**Figura 2**).

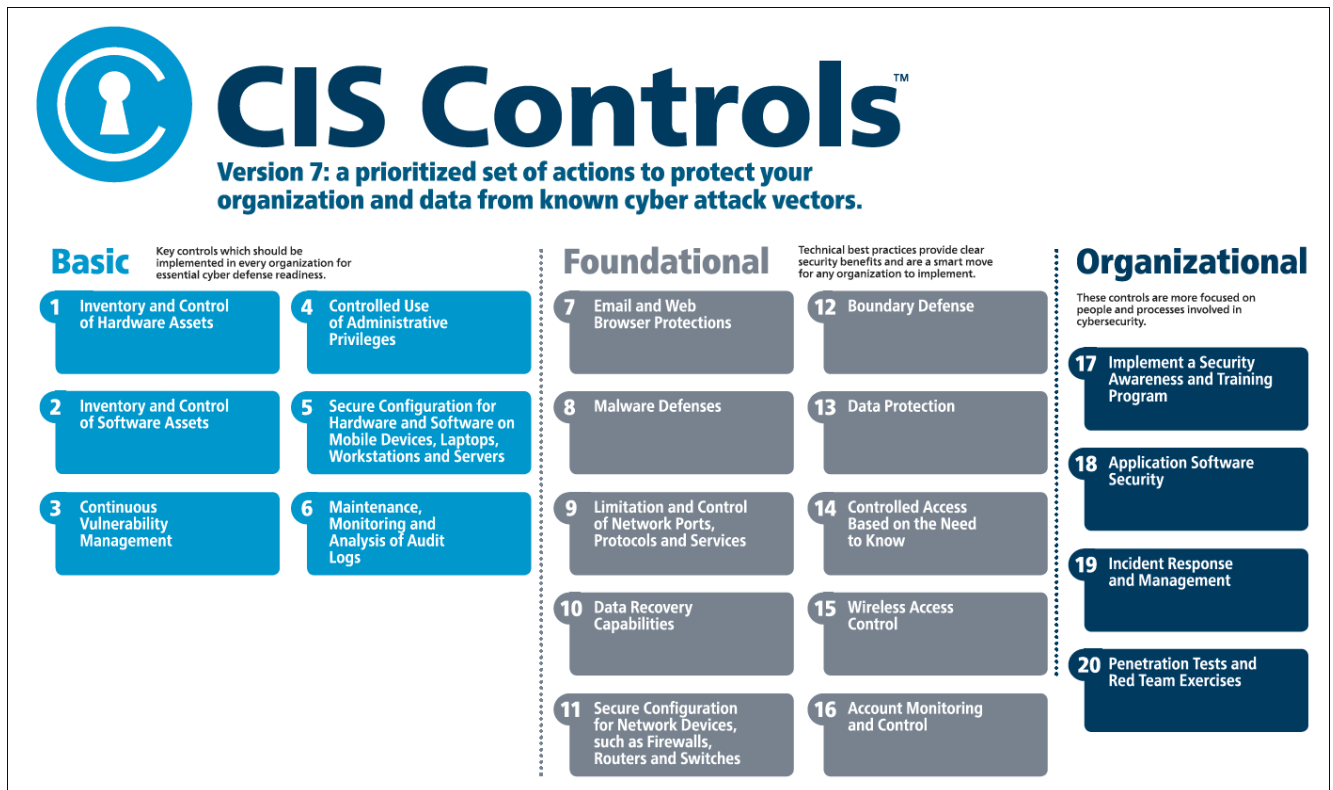


Figura 2 - 20 controles de segurança cibernética do *framework* do *Center for Internet Security* (CIS).
(Fonte: <https://www.cisecurity.org/controls/cis-controls-list>)

Também é possível que seja realizada nova auditoria sobre os procedimentos de *backup* e *restore*, porém com maior grau de profundidade do que esta.

Ademais, a organização deve se preparar, desde já, para a realização de todas as ações previstas na estratégia de atuação do TCU em segurança da informação e segurança cibernética (**Figura 1**), incluindo avaliação da implementação de controles para adequação à Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), auditoria no processo de resposta a incidentes cibernéticos e, eventualmente, fiscalização específica em algum de seus sistemas críticos.

Anexo I - Checklists para verificação de política e plano de backup

A norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação), projetada para ser usada como referência na seleção e na implementação de controles de segurança da informação comumente aceitos, fornece diretrizes para gestão nessa área, considerando os ambientes de risco das organizações.

Os *checklists* a seguir foram definidos conforme as diretrizes para implementação relacionadas no item 12.3.1 (Cópias de segurança das informações) dessa norma.

➔ Checklist para verificação de política de backup

#	VERIFICAR SE	Sim/Não/ N se aplica	OBS./ EVIDÊNCIAS
1	<u>Existe</u> uma política de <i>backup</i> (ou instrumento normativo equivalente) formalmente estabelecida		
2	A política foi <u>publicada/comunicada</u> para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
3	A política estabelece que planos/procedimentos/roteiros de <i>backup</i> de dados e de sistemas <u>específicos</u> devem ser definidos para atender as necessidades de negócio e/ou requisitos da organização		
4	A política estabelece que as cópias de segurança devem ser <u>testadas</u> regularmente por meio de testes de recuperação/restauração (<i>restore</i>), a fim de detectar eventuais falhas lógicas e físicas (nas mídias de armazenamento)		
5	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir <u>requisitos específicos de segurança da informação</u> * para as cópias de segurança realizadas (ex.: controles de acesso lógico, uso de criptografia, armazenamento em local seguro, armazenamento em local remoto seguro diferente do local original etc.) * <i>Requisitos de segurança da informação referem-se, em especial, à confidencialidade, à integridade e à disponibilidade das informações. Porém, como esses termos podem não ser citados na política, é preciso focar nos exemplos citados acima ou, então, checar se a política registra a necessidade de os controles serem compatíveis com a segurança das informações ou com a classificação das informações.</i>		
6	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir a <u>abrangência/escopo</u> das cópias de segurança de dados e de sistemas (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders etc.		
7	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir a <u>frequência</u> de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)		
8	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir os <u>tipos de cópias</u> a serem realizadas (completa/ <i>full</i> , incremental ou diferencial)		
9	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir o <u>tempo de retenção</u> das cópias de segurança, inclusive com base em requisitos legais		

➔ **Checklist para verificação de plano (ou procedimento/roteiro) de backup específico**
{especificar o nome da base de dados, arquivo de dados, sistema, aplicativo, servidor etc.}

#	VERIFICAR SE	Sim/Não/ Não se aplica	OBS./ EVIDÊNCIAS
1	O plano foi <u>publicado/comunicado</u> para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
2	O plano foi <u>aprovado</u> pelas partes interessadas		
3	O plano registra/define de modo completo e exato a <u>abrangência/escopo</u> das cópias de segurança (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) [diretrizes para implementação, alínea “a”] Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders etc.		
4	O plano estabelece que seja monitorada e <u>documentada</u> a execução do procedimento de geração das cópias de segurança, por meio de <u>registros (logs)</u> relativos a todos os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança		
5	O plano documenta os procedimentos para realizar a <u>recuperação/restauração (restore)</u> das cópias de segurança quando necessário (ou seja, o “como” recuperar os <i>backups</i>) [diretrizes para implementação, alínea “a”]		
6	O plano define a <u>frequência</u> de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.) [diretrizes para implementação, alínea “b”]		
7	O plano define os <u>tipos de cópias</u> a serem realizadas (completa, incremental ou diferencial) [diretrizes para implementação, alínea “b”]		
8	O plano define o <u>tempo de retenção</u> das cópias de segurança		
9	O plano define <u>requisitos específicos de segurança da informação*</u> (ex.: controles de acesso lógico, uso de criptografia etc.) [diretrizes para implementação, alíneas “b” e “f”] <i>* Requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações</i>		
10	O plano define a necessidade de armazenamento das cópias de segurança em <u>local seguro e em local remoto</u> seguro diferente do local original [diretrizes para implementação, alíneas “c” e “d”]		
11	O plano define procedimentos regulares de <u>teste</u> de recuperação/restauração (<i>restore</i>) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento) [diretrizes para implementação, alínea “e”]		
12	O plano estabelece que a execução dos procedimentos de <u>teste</u> de recuperação/restauração (<i>restore</i>) das cópias de segurança seja <u>documentada</u> por meio de <u>registros (logs)</u> relativos a todos os itens restaurados, a fim de detectar eventuais falhas e assegurar que houve a recuperação integral das informações		

Anexo II - Avaliação da política de *backup*

Esta avaliação consiste na aplicação do primeiro *checklist* do Anexo I ao documento anexado pelo respondente como sendo a política de *backup* da sua organização.

#	VERIFICAR SE	Sim/Não/ N se aplica	OBS./ EVIDÊNCIAS
1	Existe uma política de <i>backup</i> (ou instrumento normativo equivalente) formalmente estabelecida	S	
2	A política foi <u>publicada/comunicada</u> para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)	N/A	Não foi perguntado.
3	A política estabelece que planos/procedimentos/roteiros de <i>backup</i> de dados e de sistemas <u>específicos</u> devem ser definidos para atender as necessidades de negócio e/ou requisitos da organização		
4	A política estabelece que as cópias de segurança devem ser <u>testadas</u> regularmente por meio de testes de recuperação/restauração (<i>restore</i>), a fim de detectar eventuais falhas lógicas e físicas (nas mídias de armazenamento)		
5	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir <u>requisitos específicos de segurança da informação</u> * para as cópias de segurança realizadas (ex.: controles de acesso lógico, uso de criptografia, armazenamento em local seguro, armazenamento em local remoto seguro diferente do local original etc.) <i>* Requisitos de segurança da informação referem-se, em especial, à confidencialidade, à integridade e à disponibilidade das informações. Porém, como esses termos podem não ser citados na política, é preciso focar nos exemplos citados acima ou, então, checar se a política registra a necessidade de os controles serem compatíveis com a segurança das informações ou com a classificação das informações.</i>		
6	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir a <u>abrangência/escopo</u> das cópias de segurança de dados e de sistemas (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders etc.		
7	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir a <u>frequência</u> de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)		
8	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir os <u>tipos de cópias</u> a serem realizadas (completa/full, incremental ou diferencial)		
9	A política estabelece que os planos/procedimentos/roteiros de <i>backup</i> devem definir o <u>tempo de retenção</u> das cópias de segurança, inclusive com base em requisitos legais		

Anexo III - Avaliação do plano de *backup*

Esta avaliação consiste na aplicação do segundo *checklist* do Anexo I ao documento anexado como sendo o plano de *backup* do principal sistema da organização.

#	VERIFICAR SE	Sim/Não/ N se aplica	OBS./ EVIDÊNCIAS
1	O plano foi <u>publicado/comunicado</u> para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)	N/A	Não foi perguntado.
2	O plano foi <u>aprovado</u> pelas partes interessadas	N/A	Não foi perguntado.
3	O plano registra/define de modo completo e exato a <u>abrangência/escopo</u> das cópias de segurança (aquilo que deve ser copiado, incluindo indicações de datas/períodos) [diretrizes para implementação, alínea “a”] Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders etc.		
4	O plano estabelece que seja monitorada e <u>documentada</u> a execução do procedimento de geração das cópias de segurança, por meio de <u>registros (logs)</u> relativos a todos os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança		
5	O plano documenta os procedimentos para realizar a <u>recuperação/restauração (restore)</u> das cópias de segurança quando necessário (ou seja, o “como” recuperar os <i>backups</i>) [diretrizes para implementação, alínea “a”]		
6	O plano define a <u>frequência</u> de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.) [diretrizes para implementação, alínea “b”]		
7	O plano define os <u>tipos de cópias</u> a serem feitas (completa, incremental ou diferencial) [diretrizes para implementação, alínea “b”]		
8	O plano define o <u>tempo de retenção</u> das cópias de segurança		
9	O plano define <u>requisitos específicos de segurança da informação*</u> (ex.: controles de acesso lógico, uso de criptografia etc.) [diretrizes para implementação, alíneas “b” e “f”] * <i>Requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações</i>		
10	O plano define a necessidade de armazenamento das cópias de segurança em <u>local seguro</u> e em <u>local remoto</u> seguro diferente do local original [diretrizes para implementação, alíneas “c” e “d”]		
11	O plano define procedimentos regulares de <u>teste</u> de recuperação/restauração (<i>restore</i>) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento) [diretrizes para implementação, alínea “e”]		
12	O plano estabelece que a execução dos procedimentos de <u>teste</u> de recuperação/restauração (<i>restore</i>) das cópias de segurança seja <u>documentada</u> por meio de <u>registros (logs)</u> relativos a todos os itens restaurados, a fim de detectar eventuais falhas e assegurar que houve a recuperação integral das informações		

**Auditoria sobre a efetividade dos procedimentos
de *backup* das organizações públicas federais
(TC 036.620/2020-3)**

Relatório Comparativo de *Feedback*

Subgrupo: Admin.IV

	A classificação deste documento é de responsabilidade da organização. Entretanto, em atenção à Lei 12.527/2011 (Lei de Acesso à Informação – LAI), art. 3º, inciso I, e art. 6º, inciso I, <u>o TCU sugere que este relatório não seja classificado como sigiloso</u> e que, ao contrário, a organização o publique em seu sítio na Internet e lhe dê ampla divulgação.	
---	---	---

SUMÁRIO

1. Introdução	2
2. Seções do questionário aplicado	3
Porte da organização e política de <i>backup</i>	3
Subcontrole 1: Realize cópias de segurança (<i>backups</i>) de todos os dados da organização, de forma regular e automática	5
Subcontrole 2: Realize cópias de segurança (<i>backups</i>) integrais dos sistemas críticos da organização, de forma regular e automática	9
Subcontrole 3: Realize, periodicamente, testes de restauração (<i>restore</i>) das cópias de segurança (<i>backups</i>) da organização, de modo a atestar seu funcionamento em caso de necessidade	12
Subcontrole 4: Proteja adequadamente as cópias de segurança (<i>backups</i>) da organização, por meio de mecanismos de controle de acesso físico e lógico	15
Subcontrole 5: Armazene as cópias de segurança (<i>backups</i>) da organização em ao menos um destino não acessível remotamente	18
3. Boas práticas identificadas	20
Plano de Continuidade de Negócios (PCN)	20
Espelhamento dos bancos de dados/sistemas	20
Testes de recuperação (<i>restore</i>) aleatórios	20
Anexo I - Questionário da Auditoria sobre <i>backup</i>	21

1. Introdução

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* tornou-se fundamental para assegurar a continuidade do negócio e a consequente prestação de serviços públicos por parte dos órgãos e entidades da Administração Pública Federal (APF).

Nesse contexto, o Tribunal de Contas da União (TCU), entre os dias 15/10 e 13/11/2020, realizou auditoria, sob a relatoria do Ministro Vital do Rêgo, para avaliar se os procedimentos de *backup* e *restore* das organizações da APF, mais especificamente sobre suas principais bases de dados e sistemas críticos, são suficientes e adequados para garantir a continuidade dos serviços prestados.

A referida auditoria foi realizada no âmbito de parceria entre a Secretaria de Fiscalização de Tecnologia da Informação (Sefti) e outras doze unidades técnicas da Secretaria-Geral de Controle Externo (Segecex) do TCU, a saber: SecexAdministração, SecexAgroAmbiental, SecexDefesa, SecexEducação, SecexEstataisRJ, SecexFinanças, SecexSaúde, SecexTrabalho, SeinfraPetróleo, SeinfraPortoFerrovia, SeinfraRodoviaAviação e SeinfraUrbana.

O método utilizado foi a autoavaliação de controles internos (do inglês *Control Self-Assessment* – CSA), tendo sido disponibilizado questionário, o qual foi respondido pelos gestores de modo a refletir os controles de *backup/restore* implementados nas suas respectivas organizações, anexando-se as evidências correspondentes. Nenhuma das organizações participantes recebeu visita *in loco* e, portanto, frisa-se que as respostas constantes neste relatório são de inteira responsabilidade dos gestores respondentes dos questionários aplicados no bojo desta auditoria.

Tendo em vista o caráter eminentemente didático dessa auditoria, após a aprovação do respectivo acórdão foi enviado a cada uma das organizações auditadas relatório contendo suas respostas individuais e, onde considerado oportuno, análises efetuadas pela equipe de auditores do TCU, de modo que os gestores tivessem subsídios para aperfeiçoar as políticas e procedimentos de *backup/restore* das suas organizações, a partir da implantação gradativa das orientações e controles sugeridos.

Além do citado relatório individual, também foram elaborados relatórios comparativos para as organizações auditadas. A lógica de preparação desses relatórios envolveu a constituição de diversos subgrupos de organizações, com certa similaridade entre si, dentre o universo de órgãos e entidades que responderam o questionário da auditoria.

Desse modo, a partir da ciência da sua própria realidade (com base no relatório individual) e da possibilidade de comparar essa situação com aquela de um conjunto de organizações similares, espera-se que os gestores não apenas recebam os elementos necessários para promoverem a evolução da maturidade das suas respectivas organizações ao longo dos próximos anos, mas, também, sintam-se incentivados a fazê-lo.

Destarte, o presente relatório apresenta, então, as respostas comparativas levando em consideração o seguinte subgrupo de organizações: TSE + 26 TREs (TRE-AC não respondeu).

Todos os gráficos deste relatório foram extraídos de painel construído para essa finalidade no âmbito da auditoria. Por questões estéticas, os textos de algumas das questões foram reescritos. A íntegra do questionário aplicado, no entanto, encontra-se no Anexo I.

2. Seções do questionário aplicado

Porte da organização e política de *backup*

Quantidade total de colaboradores

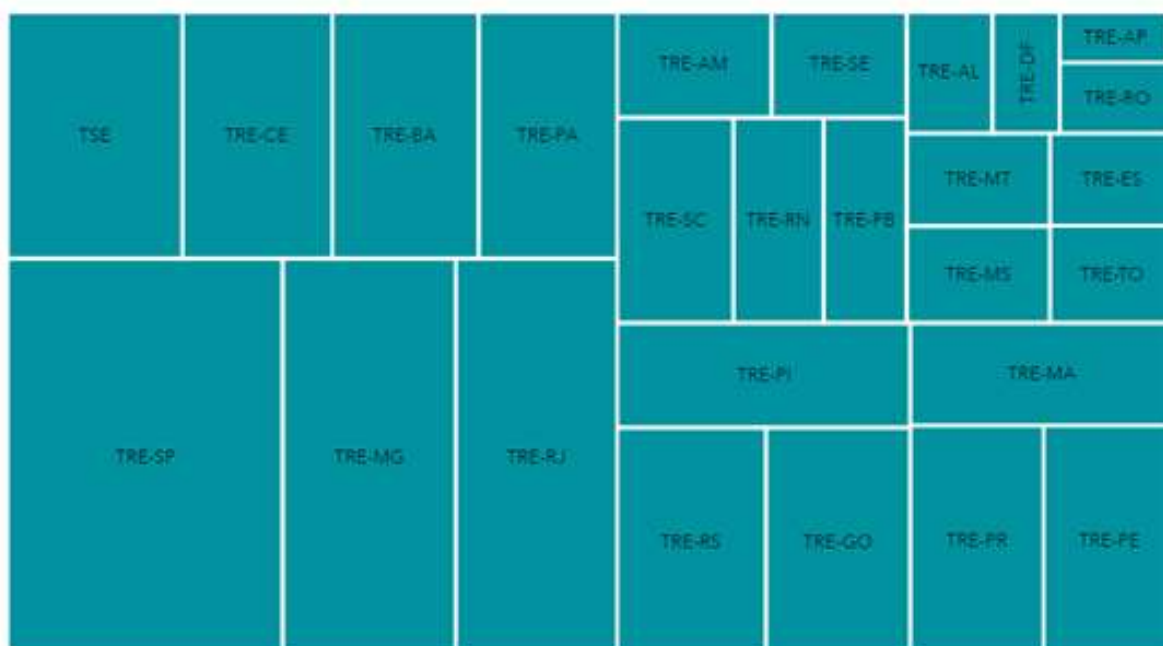


Figura 1 - Porte da organização – Quantidade total de colaboradores.

Quantidade de colaboradores do setor de TI

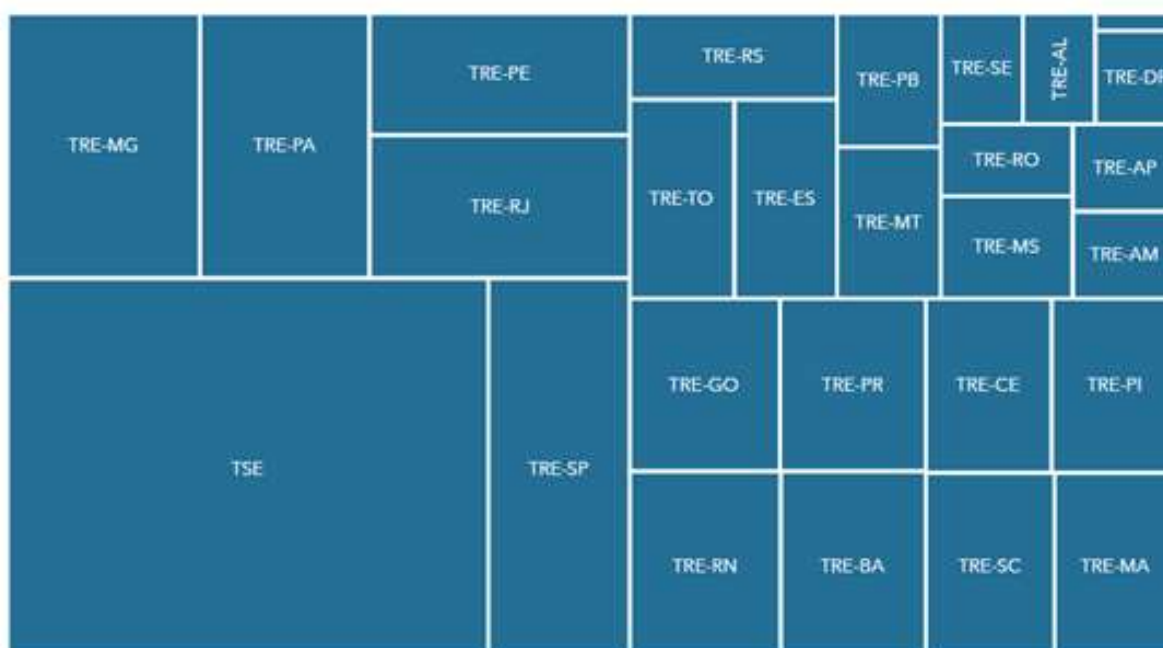


Figura 2 - Porte da organização – Quantidade de colaboradores do setor de TI.

Política de *backup*

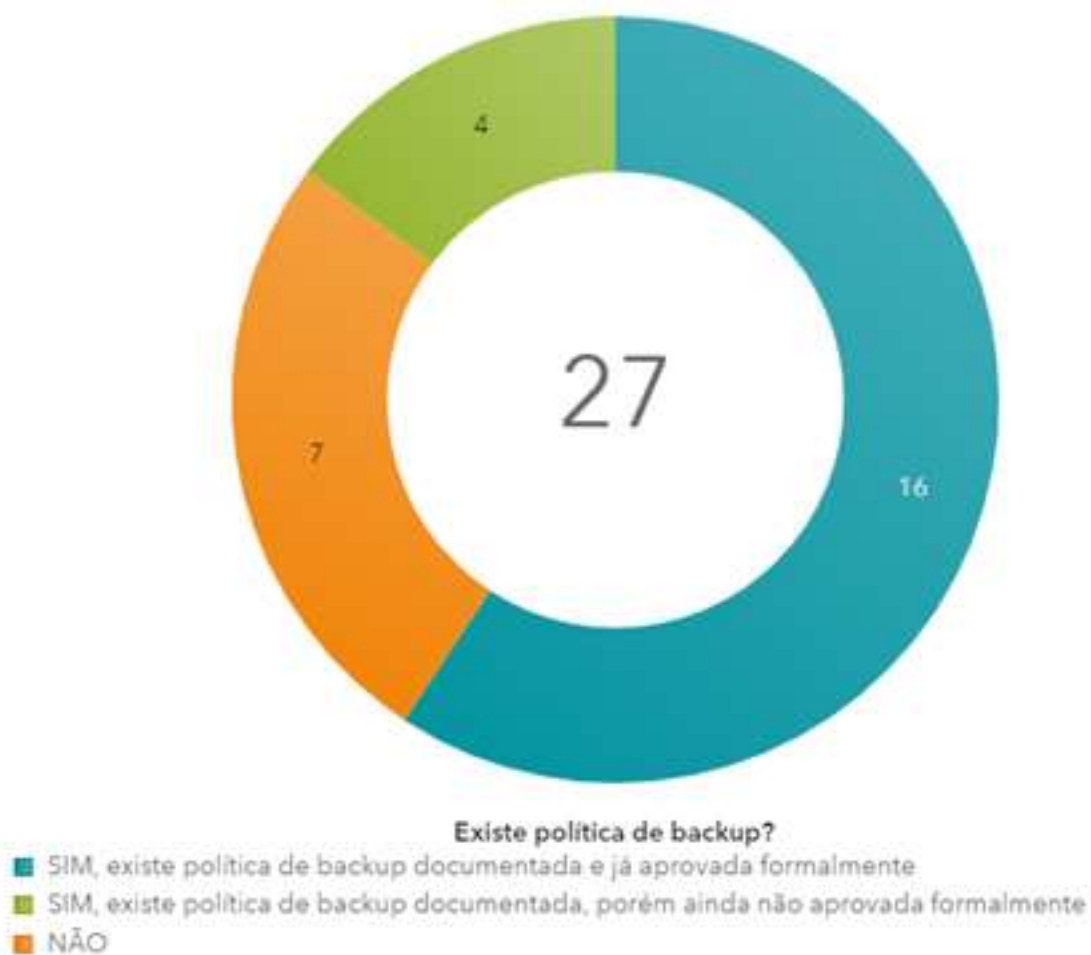


Figura 3 - Política de *backup*.

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 a auditoria avaliou a execução de cópias de segurança (*backups*) apenas em relação à principal base de dados tratada diretamente pela organização.

1.1. A organização trata diretamente alguma base de dados?



Figura 4 - Distribuição das respostas fornecidas pelas organizações à pergunta 1.1 do questionário.

1.4. Ferramenta(s) utilizada(s) para gerenciar os *backups* da principal base de dados



Figura 5 - Nuvem com os tamanhos das palavras proporcionais ao número de vezes que foram citadas nas respostas fornecidas pelas organizações à pergunta 1.4 do questionário.

1.5.1. Periodicidade dos *backups* completos (*full*) da principal base de dados

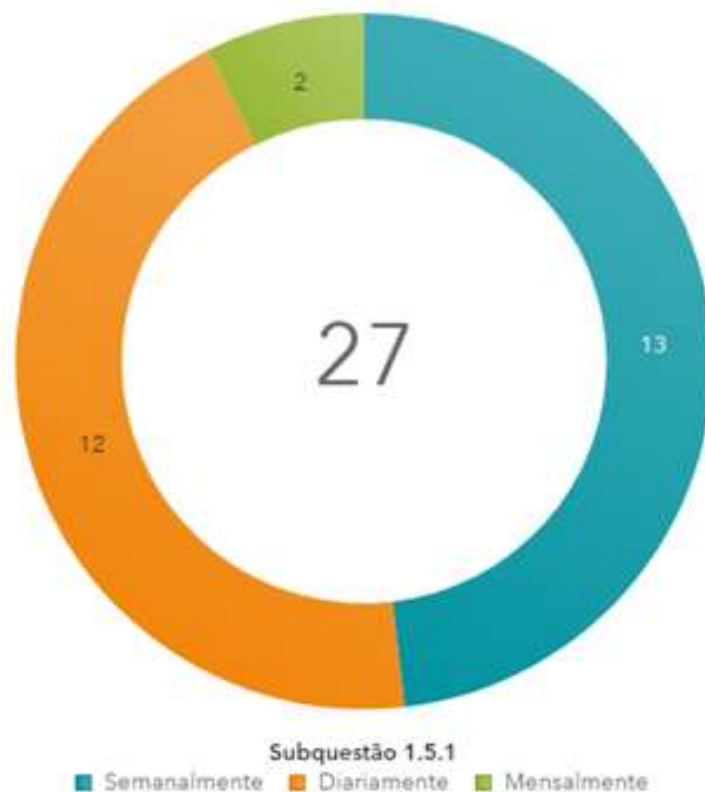


Figura 6 - Distribuição das respostas fornecidas pelas organizações à pergunta 1.5.1 do questionário.

1.5.2. Periodicidade dos *backups* diferenciais da principal base de dados

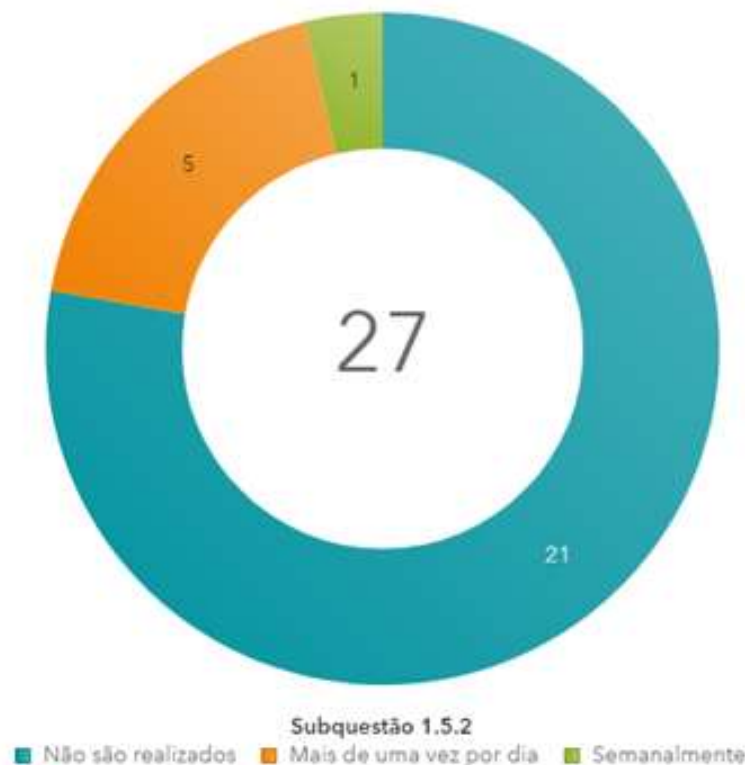


Figura 7 - Distribuição das respostas fornecidas pelas organizações à pergunta 1.5.2 do questionário.

1.5.3. Periodicidade dos *backups* incrementais da principal base de dados

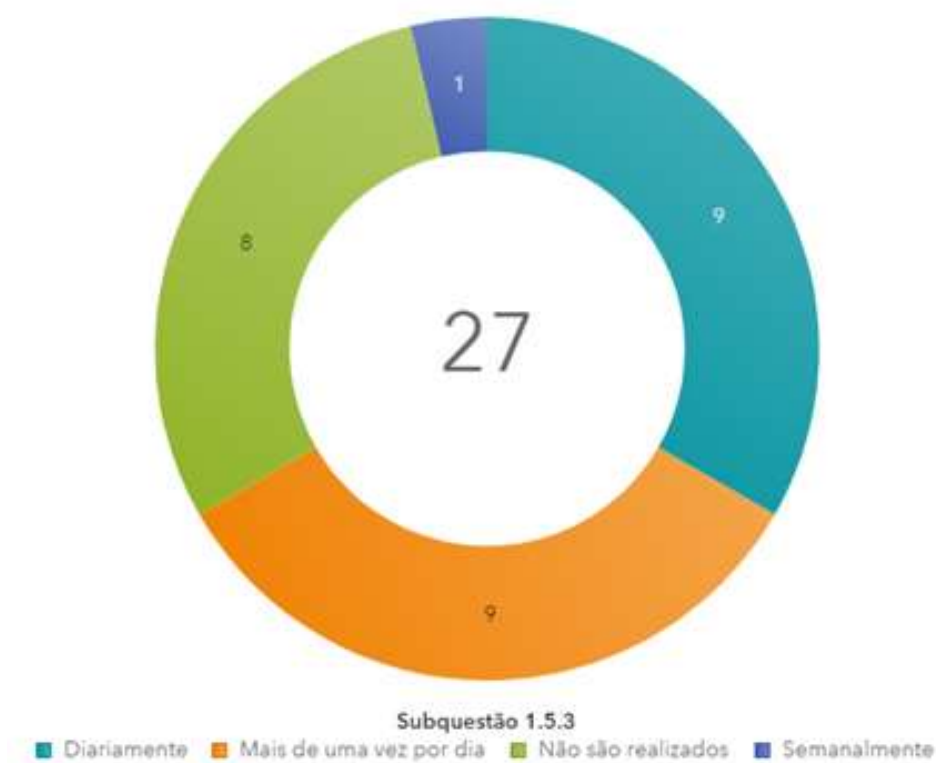


Figura 8 - Distribuição das respostas fornecidas pelas organizações à pergunta 1.5.3 do questionário.

1.6. Forma de realização dos *backups* completos (*full*) da principal base de dados



Figura 9 - Distribuição das respostas fornecidas pelas organizações à pergunta 1.6 do questionário.

Subcontrole 2: Realize cópias de segurança (*backups*) integrais dos sistemas críticos da organização, de forma regular e automática

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 o desempenho 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 a auditoria avaliou a execução de cópias de segurança (*backups*) integrais apenas 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?

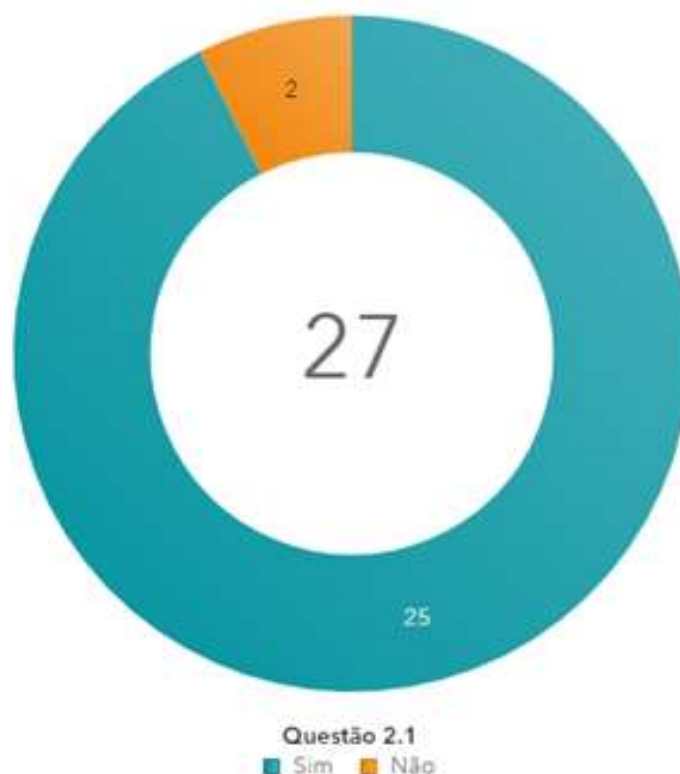


Figura 10 - Distribuição das respostas fornecidas pelas organizações à pergunta 2.1 do questionário.

2.3. Ferramenta(s) utilizada(s) para gerenciar os *backups* do principal sistema



Figura 11 - Nuvem com os tamanhos das palavras proporcionais ao número de vezes que foram citadas nas respostas fornecidas pelas organizações à pergunta 2.3 do questionário.

2.4. Periodicidade dos *backups* do principal sistema

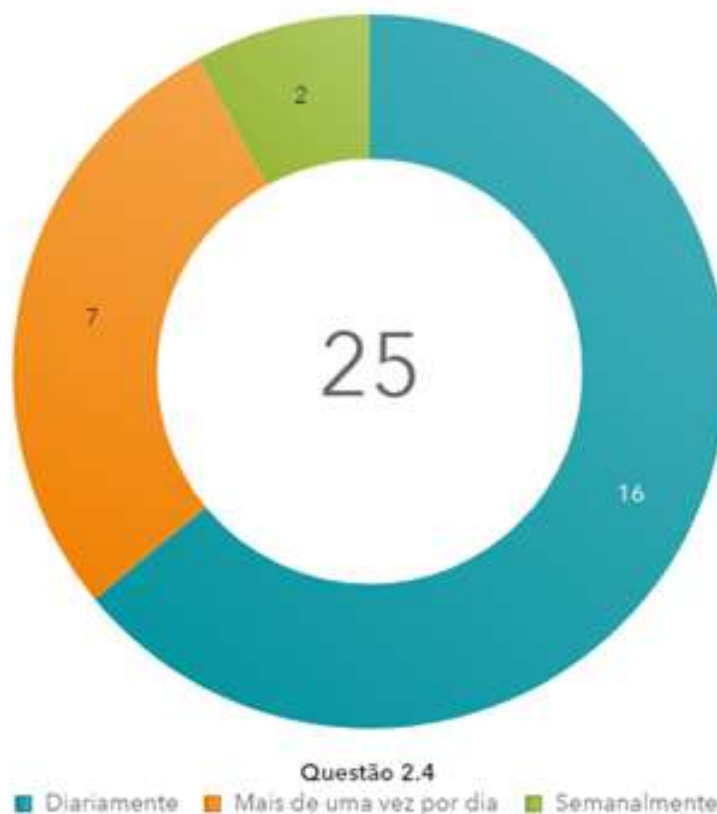


Figura 12 - Distribuição das respostas fornecidas pelas organizações à pergunta 2.4 do questionário.

2.5. Forma de realização dos *backups* do principal sistema

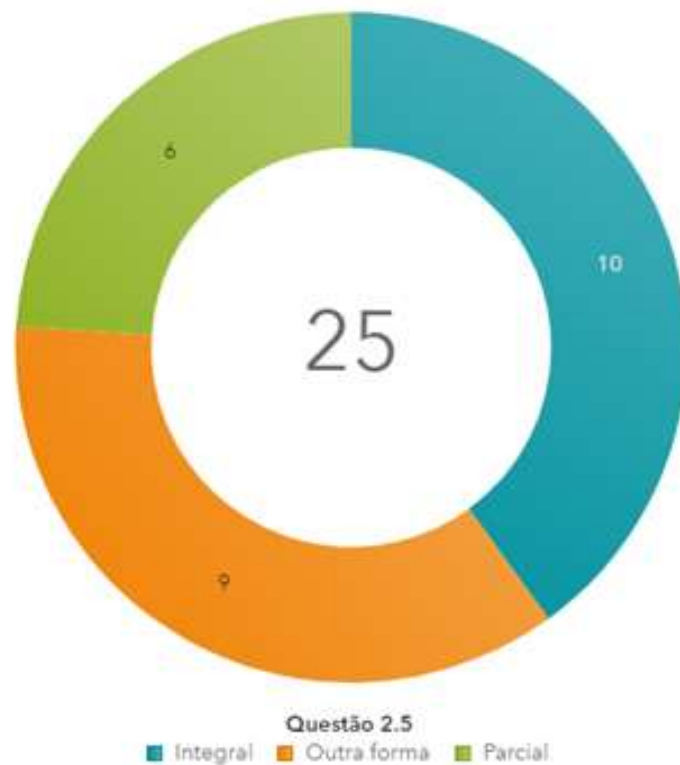


Figura 13 - Distribuição das respostas fornecidas pelas organizações à pergunta 2.5 do questionário.

2.7. A organização possui plano de *backup* específico para o principal sistema?

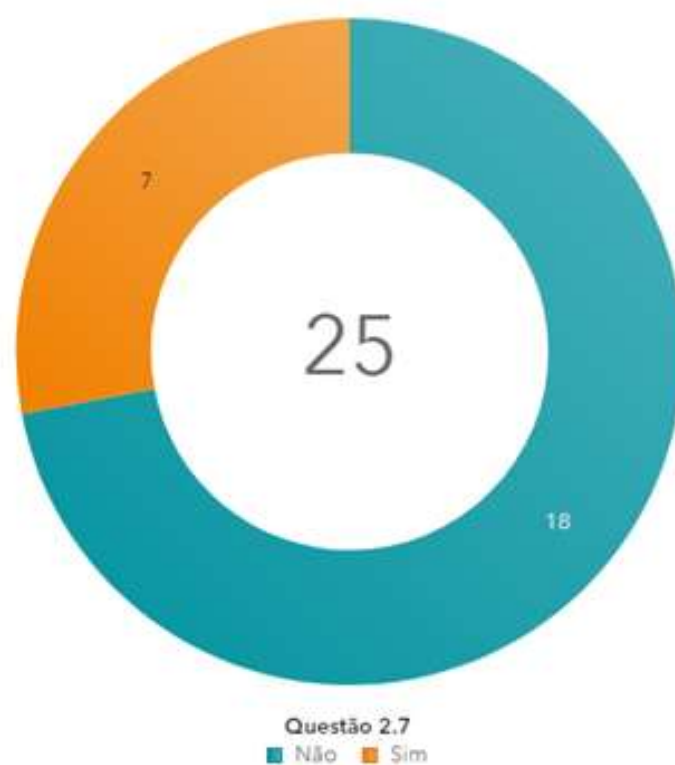


Figura 14 - Distribuição das respostas fornecidas pelas organizações à pergunta 2.7 do questionário.

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 a auditoria avaliou a execução do procedimento de restauração (*restore*) apenas 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?



Figura 15 - Distribuição das respostas fornecidas pelas organizações à pergunta 3.1 do questionário.

3.2. Os testes de restauração (*restore*) são documentados?

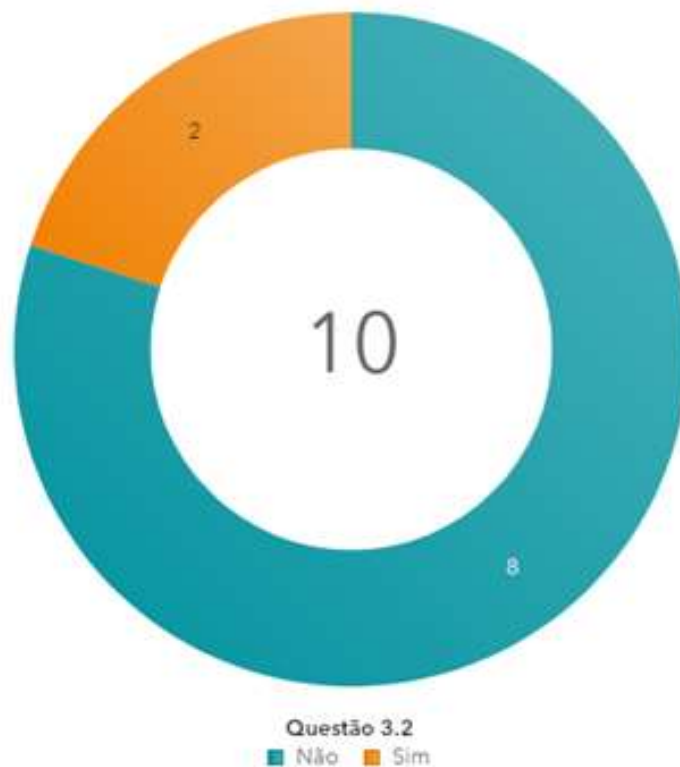


Figura 16 - Distribuição das respostas fornecidas pelas organizações à pergunta 3.2 do questionário.

3.4.1. Periodicidade dos testes de restauração (*restore*) da principal base de dados

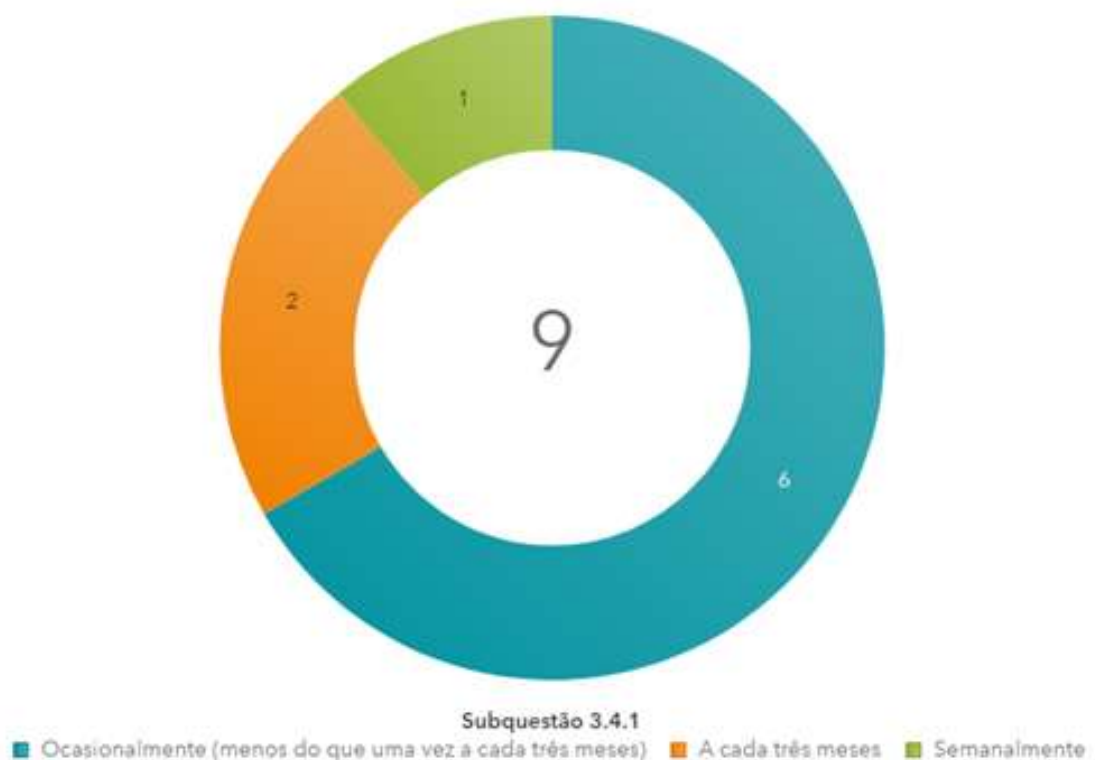


Figura 17 - Distribuição das respostas fornecidas pelas organizações à pergunta 3.4.1 do questionário.

3.4.2. Periodicidade dos testes de restauração (*restore*) do principal sistema

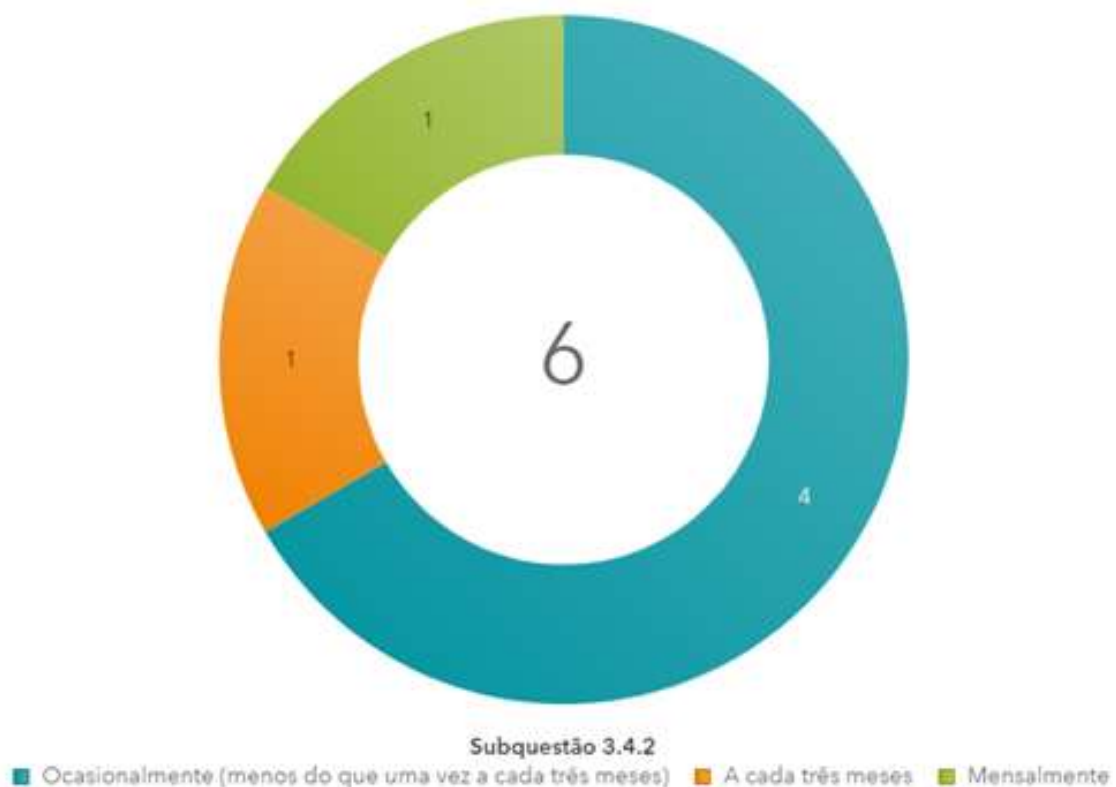


Figura 18 - Distribuição das respostas fornecidas pelas organizações à pergunta 3.4.2 do questionário.

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 a auditoria avaliou 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, considerou serem 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. Local de armazenamento dos arquivos de *backup*



Figura 19 - Distribuição das respostas fornecidas pelas organizações à pergunta 4.1 do questionário.

4.4. Utilização de criptografia no local de armazenamento dos arquivos de *backup*

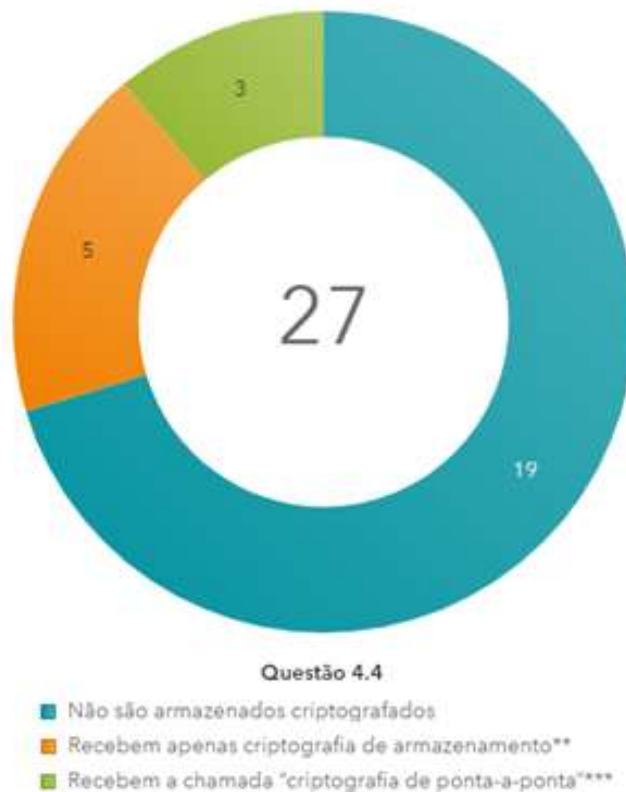


Figura 20 - Distribuição das respostas fornecidas pelas organizações à pergunta 4.4 do questionário.

4.5. Controle de acesso físico no local de armazenamento dos arquivos de *backup*

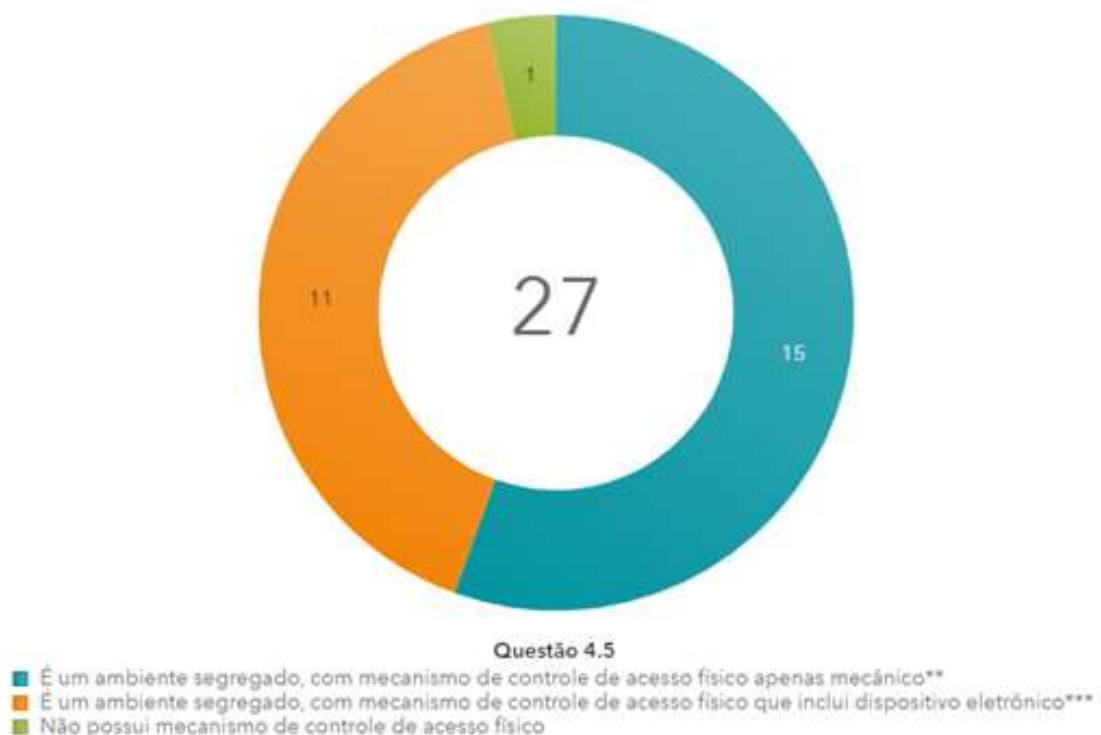


Figura 21 - Distribuição das respostas fornecidas pelas organizações à pergunta 4.5 do questionário.

4.6. O acesso ao ambiente segregado é concedido a partir de algo que somente o usuário

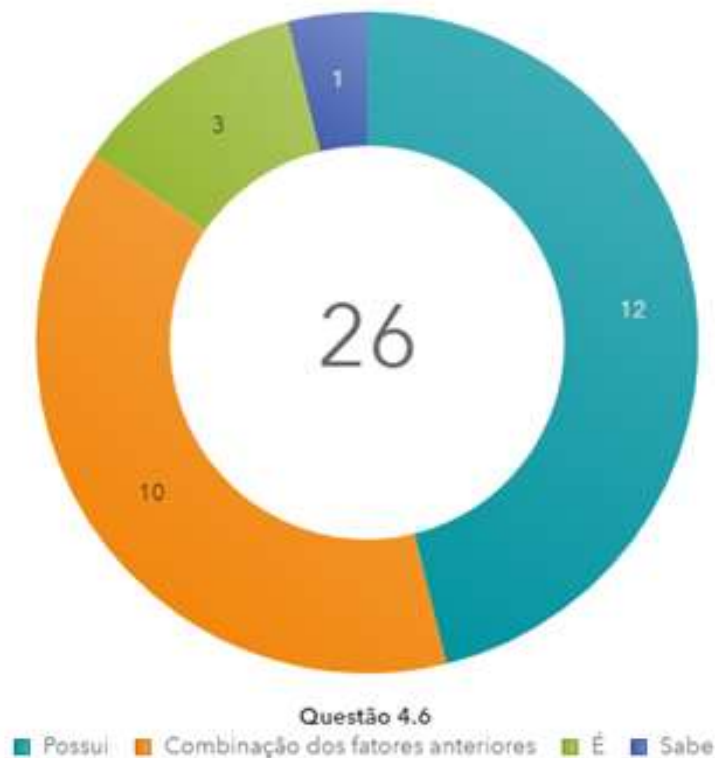


Figura 22 - Distribuição das respostas fornecidas pelas organizações à pergunta 4.6 do questionário.

4.8. Os acessos ao ambiente segregado são registrados?

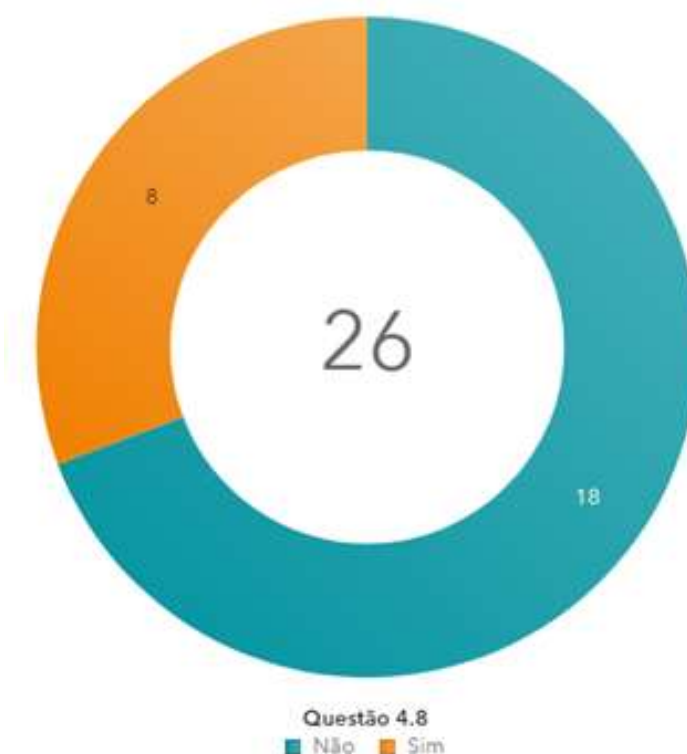


Figura 23 - Distribuição das respostas fornecidas pelas organizações à pergunta 4.8 do questionário.

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 a auditoria avaliou 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 os *backups* em ao menos um destino não acessível remotamente?

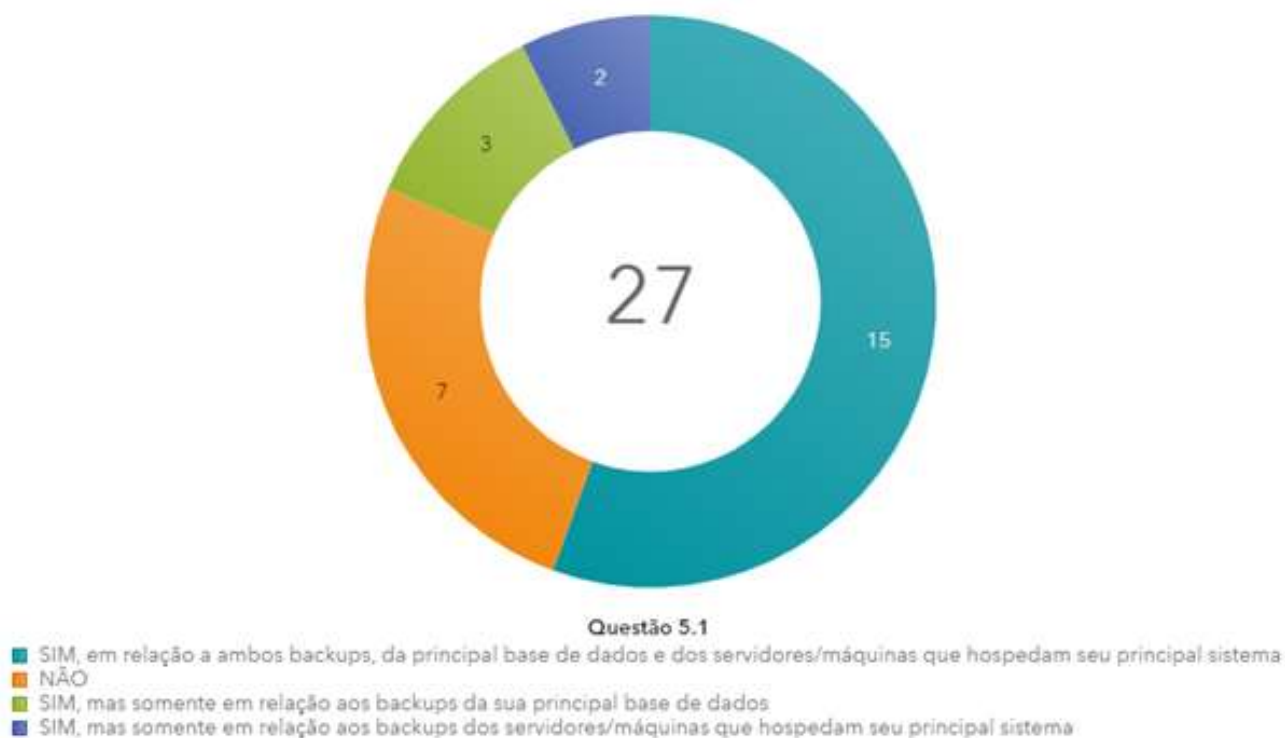


Figura 24 - Distribuição das respostas fornecidas pelas organizações à pergunta 5.1 do questionário.

5.2. Mídia não acessível remotamente com os *backups* da principal base de dados



Figura 25 - Distribuição das respostas fornecidas pelas organizações à pergunta 5.2 do questionário.

5.3. Mídia não acessível remotamente com os *backups* do principal sistema



Figura 26 - Distribuição das respostas fornecidas pelas organizações à pergunta 5.3 do questionário.

3. Boas práticas identificadas

Plano de Continuidade de Negócios (PCN)

A norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação), em seu item 17 (Aspectos da segurança da informação na gestão da continuidade do negócio), traz diversos controles e diretrizes relacionados ao planejamento, à implementação e à constante avaliação da continuidade da segurança da informação de uma organização, incluindo a implementação de redundâncias com vistas a atender requisitos de disponibilidade.

Mais especificamente, a norma ABNT NBR 15999-1:2007 (Gestão de continuidade de negócios – Parte 1: Código de prática) detalha a gestão da continuidade de negócios (GCN), processo que agrega valor a qualquer organização, visto que, independentemente do porte, todas estão sujeitas à eventual ocorrência de interrupções, pelas mais diversas razões (falhas tecnológicas, desastres naturais, problemas no fornecimento de serviços públicos, incidentes de segurança, ataques cibernéticos e até atos de terrorismo).

Assim sendo, identificou-se como boa prática a manutenção de Planos de Continuidade de Negócios (PCN), incluindo, em alguns casos, a previsão de medidas de contingência voltadas especificamente a assegurar a continuidade da operação de determinados sistemas/plataformas tecnológicas, a exemplo da realização de procedimentos de recuperação (*restore*) de cópias de segurança (*backups*), quando necessário.

Entre outros itens, tais planos devem especificar quem são os responsáveis em casos de crise e seus contatos, prever os eventos de diferentes graus de gravidade/dano e delinear ações de contingência e roteiros de resposta para cada um desses cenários (“ação”, “quem”, “onde”, “como” e “resultado esperado”). Com isso, caso se materialize algum dos sinistros previstos, a organização já tem definidos e treinados os respectivos responsáveis, bem como os procedimentos a serem realizados, diminuindo, conseqüentemente, o tempo de reação e mitigando os prejuízos advindos desses episódios.

Espelhamento dos bancos de dados/sistemas

Além das ferramentas usuais de *backup*, o uso de bancos de dados e servidores espelhados, em tempo real, também diminui os tempos de reação e de retorno à atividade “normal” na eventual ocorrência de sinistro, tendo em vista que, por exemplo, nos casos de falha, o banco de dados/máquina/servidor espelhado pode ser programado para assumir a operação quase que instantaneamente no lugar do ativo principal. Essa prática é especialmente útil para as organizações que possuem volumes menores de dados.

Testes de recuperação (*restore*) aleatórios

Pode ser proibitivamente caro, ou mesmo inviável, realizar testes de recuperação (*restore*) periódicos sobre todas as bases de dados, arquivos e sistemas da organização, sobretudo à medida que se reduz a frequência de realização desses testes.

Assim, diversas organizações “sorteiam” as bases de dados/sistemas a serem testados em cada período, em regime de rodízio, assegurando, com isso, que, com alguma periodicidade, pelo menos, todas(os) sejam testados.

Anexo I - Questionário da Auditoria sobre *backup*

A seguir, são listadas as perguntas do questionário aplicado aos gestores das organizações relacionadas na “Introdução”, cuja consolidação das respectivas respostas resultou na elaboração deste relatório.

 **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 (clique 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.**

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*.**

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 gestão 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*.**



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 (clique 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 (clique 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*.**

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 adequa(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 (clique 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 (clique 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*.

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.