TRIBUNAL DE CONTAS DA UNIÃO

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

Relatório Individual de Autoavaliação

TRF1
Tribunal Regional Federal da 1ª Região

	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, o TCU sugere que este relatório não seja classificado como sigiloso e que, ao contrário, a organização o publique em seu sítio na Internet e lhe dê ampla divulgação.	

SUMÁRIO

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**).

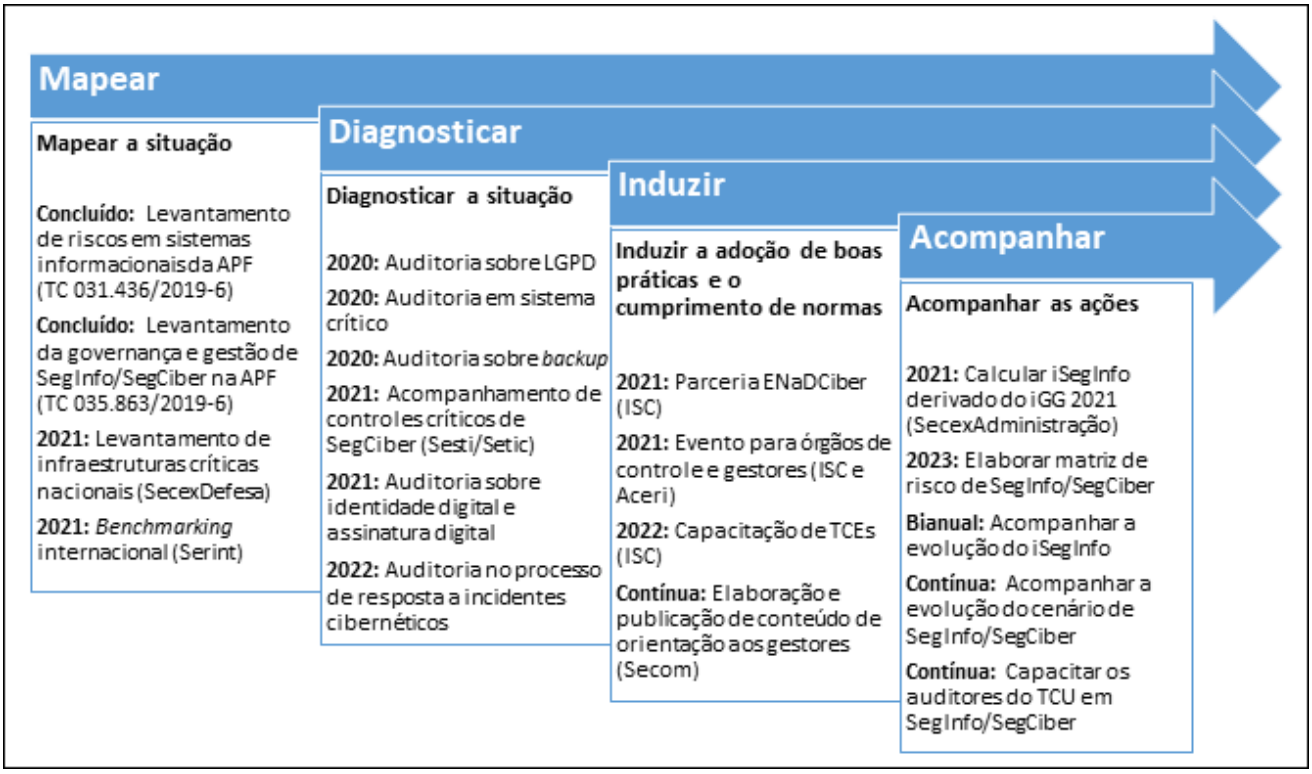


Figura 1 - Estratégia de atuação do TCU em segurança da informação e segurança cibernética.
(Fonte: elaboração própria)

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:	TRF1
Nome:	Tribunal Regional Federal da 1ª Região
Quantidade de colaboradores:	1600
Quantidade de colaboradores que atuam no setor de TI:	103
Dados do servidor que respondeu o questionário	
Nome completo:	Lucio Melre da Silva
CPF:	35172045104
Cargo:	Diretor da Secretaria de Tecnologia da Informação

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?
SIM, existe política de backup documentada e já aprovada formalmente

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).

O Anexo II contém a avaliação da política de *backup* desta organização.

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/ Ñ se aplica	OBS./ EVIDÊNCIAS
1	Existe uma política de *backup* (ou instrumento normativo equivalente) formalmente estabelecida	S	
2	A política foi publicada/comunicada 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 *backup* de dados e de sistemas específicos devem ser definidos para atender as necessidades de negócio e/ou requisitos da organização	S	Portaria Presi – 10264108, arts. 7º, 9º e 10, *caput*, e Parágrafo único
4	A política estabelece que as cópias de segurança devem ser testadas regularmente por meio de testes de recuperação/restauração (*restore*), a fim de detectar eventuais falhas lógicas e físicas (nas mídias de armazenamento)	S	Portaria Presi – 10264108, art. 29
5	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir requisitos específicos de segurança da informação* paras 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.) ** 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.*	S	Portaria Presi – 10264108, art. 27 Obs: não contempla controles de acesso lógico, uso de criptografia
6	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir a abrangência/escopo 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.	S	Portaria Presi – 10264108, arts. 9º e 10, *caput*, e Parágrafo único
7	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)	S	Portaria Presi – 10264108, art. 13, I a IV
8	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir os tipos de cópias a serem realizadas (completa/*full*, incremental ou diferencial)	S	Portaria Presi – 10264108, art. 18, II
9	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir o tempo de retenção das cópias de segurança, inclusive com base em requisitos legais	S	Portaria Presi – 10264108, arts. 14, I a IV, e 16, I a IV

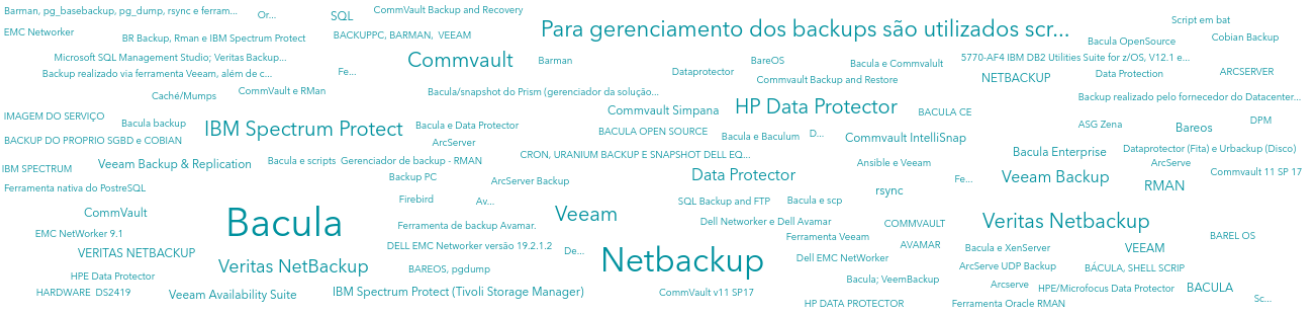
Subcontrole 1: Realize cópias de segurança (*backups*) de todos os dados da organização, de forma regular e automática

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:	
Base de dados oracle (sistemas judiciais e administrativos)	
1.3. Qual é o tamanho aproximado, em MB, da principal base de dados tratada diretamente pela organização?	
12000000	
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:	
Netbackup	
1.5. Em relação à base de dados referida na pergunta 1.2, com qual periodicidade são realizados *backups*:	
Completos (full)?	Semanalmente
Diferenciais?	Não são realizados
Incrementais?	Diariamente
1.6. Indique a forma de realização dos *backups* completos da base de dados referida na pergunta 1.2:	
Automatizada	
1.7. Solicitaçao 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.



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?
Sim
2.2. Identifique o principal sistema hospedado pela organização:
Sistema Processual (Juris)
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:
Netbackup
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*:
Diariamente
2.5. Indique a forma de realização dos *backups* do servidor ou conjunto de servidores/máquinas:
Parcial. O backup diário é incremental. Os backups semanais e mensais são full. A resposta dada a esta questão (parcial) se refere ao backup diário.
2.6. Solicitaçao de evidência.
2.7. A organização possui plano de *backup* para o sistema referido na pergunta 2.2?

Não

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*?	
NÃO	
3.2 Os testes de restauração (*restore*) são documentados (isto é, geram algum tipo de registro formal ou relatório de resultados)?	
N/A	
3.3. Solicitaçao 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?	
Dos servidores/máquinas que hospedam o sistema referido na pergunta 2.2?	
3.5. Solicitaçao de evidência.	
3.6. Solicitaçao 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. Solicitaçao 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. Solicitaçao 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?
SIM, em relação a ambos backups, da principal base de dados e dos servidores/máquinas que hospedam seu principal sistema
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)?
Fita. O backup de dados é realizado de todo o banco (oracle). Não é realizado backup por sistemas.
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)?
Fita
5.4. Solicitaçao de evidência.
5.5. Solicitaçao 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 (*backups*) de todos os dados da organização, de forma regular e automática	7
Subcontrole 2: Realize cópias de segurança (*backups*) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade	5
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	2
Subcontrole 4: Proteja adequadamente as cópias de segurança (*backups*) da organização, por meio de mecanismos de controle de acesso físico e lógico	6
Subcontrole 5: Armazene as cópias de segurança (*backups*) da organização em ao menos um destino não acessível remotamente	10

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:
O TRF 1ª Região é responsável pelo desenvolvimento e sustentação de todos os sistemas do tribunal e Seções Judiciárias vinculadas, bem como a gestão de infraestrutura. A JF1 (Justiça Federal da 1ª Região) é composta por 96 unidades, dentre Seções Judiciárias, Subseções Judiciárias e o próprio Tribunal. Nas Seções Judiciárias, em número de quatorze, são realizadas cópias de dados dos sistemas locais, sob a responsabilidade de gestores locais. As respostas dadas a este questionário se referem apenas ao sítio do TRF1, localizado em Brasília.

O respondente enfatiza que o TRF 1ª Região é responsável pelo desenvolvimento e sustentação de todos os sistemas do tribunal e Seções Judiciárias vinculadas, bem como a gestão de infraestrutura. Ademais, evidencia que as respostas dadas a este questionário se referem apenas ao sítio do TRF1, localizado em Brasília.

Além disso, o respondente reconheceu as deficiências da organização quanto a quase todos os subcontroles, exetuando-se o subcontrole 5.

No entanto, entende-se que houve uma incongruência em relação aos Subcontroles 3 e 4, uma vez que o TRF 1 não realiza testes periódicos de restauração e bem como não possui

localidade remota onde são armazenados os *backups*, não possui a chamada “criptografia de ponta-a-ponta, não possui instalado um dispositivo eletrônico na entrada do ambiente segregado, nem tampouco implementou o registro de controle de acesso ao ambiente segregado.

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**).

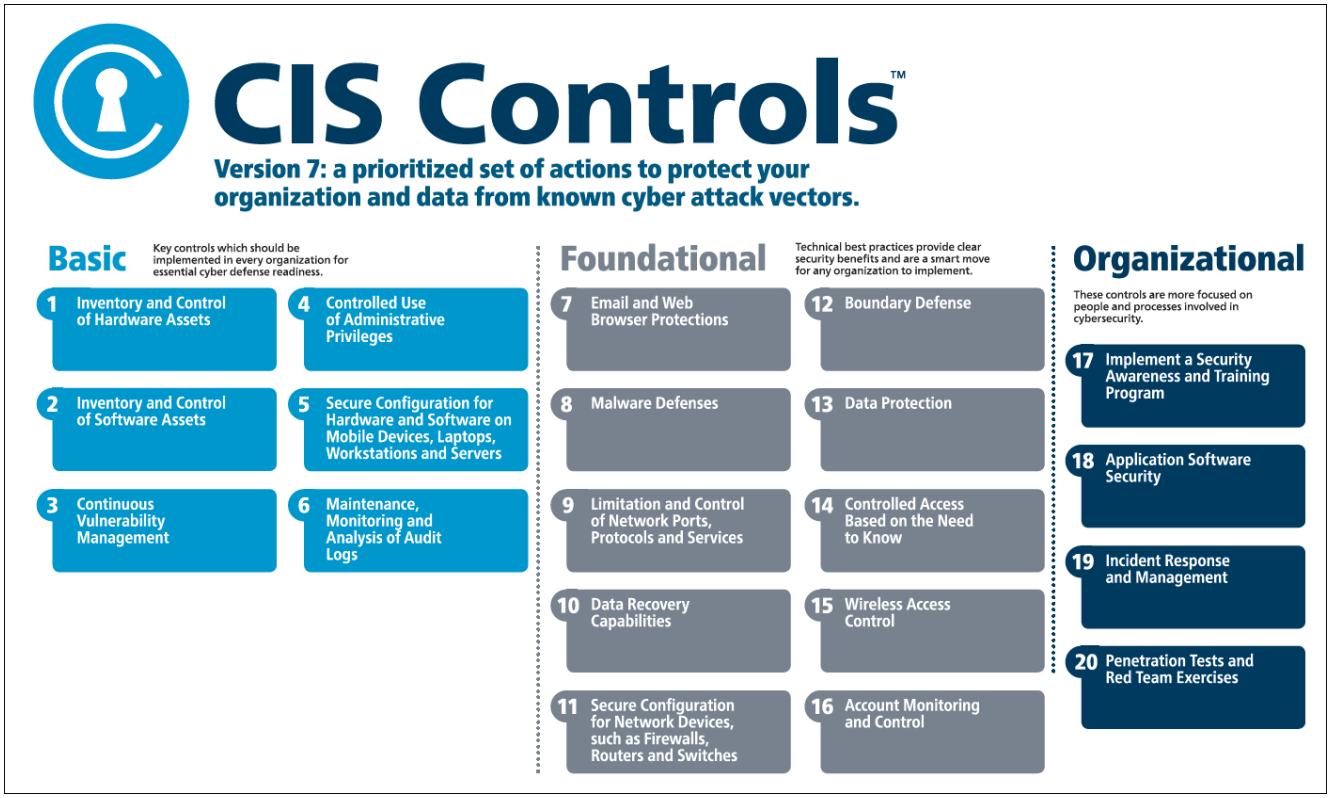


Figura 2 - 20 controles de segurança cibernética do *framework* do *Center for Internet Security* (CIS).
(Fonte: https://www.cisecurity.org/controls/cis-controls-list)

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/ Ñ se aplica	OBS./ EVIDÊNCIAS
1	Existe uma política de *backup* (ou instrumento normativo equivalente) formalmente estabelecida		
2	A política foi publicada/comunicada para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
3	A política estabelece que planos/procedimentos/roteiros de *backup* de dados e de sistemas específicos 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 testadas regularmente por meio de testes de recuperação/restauração (*restore*), a fim de detectar eventuais falhas lógicas e físicas (nas mídias de armazenamento)		
5	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir requisitos específicos de segurança da informação* paras 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.) ** 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.*		
6	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir a abrangência/escopo 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 *backup* devem definir a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)		
8	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir os tipos de cópias a serem realizadas (completa/*full*, incremental ou diferencial)		
9	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir o tempo de retenção 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/ Ñ se aplica	OBS./ EVIDÊNCIAS
1	O plano foi publicado/comunicado para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
2	O plano foi aprovado pelas partes interessadas		
3	O plano registra/define de modo completo e exato a abrangência/escopo 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 documentada a execução do procedimento de geração das cópias de segurança, por meio de registros (*logs*) 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 recuperação/restauração (*restore*) das cópias de segurança quando necessário (ou seja, o "como" recuperar os *backups*) [diretrizes para implementação, alínea "a"]		
6	O plano define a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.) [diretrizes para implementação, alínea "b"]		
7	O plano define os tipos de cópias a serem realizadas (completa, incremental ou diferencial) [diretrizes para implementação, alínea "b"]		
8	O plano define o tempo de retenção das cópias de segurança		
9	O plano define requisitos específicos de segurança da informação* (ex.: controles de acesso lógico, uso de criptografia etc.) [diretrizes para implementação, alíneas "b" e "f"] * *Requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações*		
10	O plano define a necessidade de armazenamento das cópias de segurança em local seguro e em local remoto seguro diferente do local original [diretrizes para implementação, alíneas "c" e "d"]		
11	O plano define procedimentos regulares de teste de recuperação/restauração (*restore*) 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 teste de recuperação/restauração (*restore*) das cópias de segurança seja documentada por meio de registros (*logs*) 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/ Ñ se aplica	OBS./ EVIDÊNCIAS
1	Existe uma política de *backup* (ou instrumento normativo equivalente) formalmente estabelecida	S	
2	A política foi publicada/comunicada 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 *backup* de dados e de sistemas específicos 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 testadas regularmente por meio de testes de recuperação/restauração (*restore*), a fim de detectar eventuais falhas lógicas e físicas (nas mídias de armazenamento)		
5	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir requisitos específicos de segurança da informação* paras 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.) ** 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.*		
6	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir a abrangência/escopo 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 *backup* devem definir a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)		
8	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir os tipos de cópias a serem realizadas (completa/*full*, incremental ou diferencial)		
9	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir o tempo de retenção 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/ Ñ se aplica	OBS./ EVIDÊNCIAS
1	O plano foi publicado/comunicado para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)	N/A	Não foi perguntado.
2	O plano foi aprovado pelas partes interessadas	N/A	Não foi perguntado.
3	O plano registra/define de modo completo e exato a abrangência/escopo 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 documentada a execução do procedimento de geração das cópias de segurança, por meio de registros (*logs*) 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 recuperação/restauração (*restore*) das cópias de segurança quando necessário (ou seja, o "como" recuperar os *backups*) [diretrizes para implementação, alínea "a"]		
6	O plano define a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.) [diretrizes para implementação, alínea "b"]		
7	O plano define os tipos de cópias a serem feitas (completa, incremental ou diferencial) [diretrizes para implementação, alínea "b"]		
8	O plano define o tempo de retenção das cópias de segurança		
9	O plano define requisitos específicos de segurança da informação* (ex.: controles de acesso lógico, uso de criptografia etc.) [diretrizes para implementação, alíneas "b" e "f"] * *Requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações*		
10	O plano define a necessidade de armazenamento das cópias de segurança em local seguro e em local remoto seguro diferente do local original [diretrizes para implementação, alíneas "c" e "d"]		
11	O plano define procedimentos regulares de teste de recuperação/restauração (*restore*) 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 teste de recuperação/restauração (*restore*) das cópias de segurança seja documentada por meio de registros (*logs*) relativos a todos os itens restaurados, a fim de detectar eventuais falhas e assegurar que houve a recuperação integral das informações		