FUNPRESP-JUD
Fundação de Previdência Complementar do
Servidor Público Federal do Poder Judiciário

PROGRAMA DE CONTROLE INTERNO – PCI

Procedimentos de Armazenamento e Segurança de Dados

Dezembro 2015

FUNPRESP-JUD
Fundação de Previdência Complementar do
Servidor Público Federal do Poder Judiciário

SUMÁRIO

INTRODUÇÃO

Este Relatório tem por objetivo avaliar os procedimentos de Armazenamento e Segurança de Dados, verificando a confidencialidade, disponibilidade e integridade das informações.

Mencionado monitoramento está previsto no **Programa de Controle Interno – PCI 2014-2015**, aprovado na 36ª Reunião Ordinária da Diretoria Executiva em 15/09/2014, construído a partir de pontos identificados e avaliados ponderando-se a probabilidade de ocorrência e sua consequência (impacto).

O **PCI** traz os critérios para a avaliação das áreas internas e das atividades da Fundação de Previdência Complementar do Servidor Público Federal do Poder Judiciário - Funpresp-Jud a serem monitoradas com prioridade no âmbito de um programa de controle interno.

O controle de processos e procedimentos internos objetiva a prevenção de riscos e será cumprido pelo acompanhamento contínuo com foco nas atividades e nos resultados mais significativos da Entidade.

Nesse panorama foi construída a primeira **Matriz de Risco** (resumo das principais atividades), mecanismo por meio do qual foi possível selecionar as prioridades de controle nesta fase inicial da Funpresp-Jud, de acordo com os indicadores de vulnerabilidade (probabilidade de ocorrência e consequência).

O desenvolvimento de uma cultura de controles internos e da gestão de riscos em todos os níveis hierárquicos é considerado uma boa prática no segmento de Previdência Complementar. Nesse sentido, indicou a Auditoria dos Patrocinadores no relatório emitido em 2014 (item 3.5.1):

> *"Realizar trabalho específico com objetivo de mensurar a efetiva implantação e o grau de funcionamento dos controles internos da entidade, encaminhando os resultados apurados ao Conselho Fiscal."*

Esse trabalho específico de mensuração demandará uma avaliação direta nas áreas, inclusive uma autoavaliação, examinando suas rotinas e respectivos controles aplicados diretamente pelas unidades, e demais monitoramentos supervenientes.

1. METODOLOGIA

As atividades de monitoramento da área de **Tecnologia e Informação - TI** foram realizadas no ambiente interno da Fundação, cujo método de trabalho consistiu em questionário de avaliação, resultando em um Plano de Recomendações.

Essa atividade de controle interno foi realizada com base nas melhoras práticas de governança, de acordo com as normas estabelecidas pelo COBIT e pela ISO/IEC 27001, que estabelece um padrão para sistema de gestão da segurança da informação.

Os principais fatores analisados foram políticas e processos formais, controle de acessos, gestão de incidentes de segurança da informação, gestão de contratos, armazenamento e cópia de segurança dos dados (backups) e segurança/antivírus.

2. QUESTIONÁRIO DE AVALIAÇÃO

Transcreve-se abaixo o questionário respondido pela Coordenadoria de Tecnologia da Informação:

Políticas e Processos formais

1. **Existe política de segurança da informação formalmente aprovada?**
   Não. No PDTI da Fundação há previsão para apresentação de política de segurança até dezembro de 2015.

2. **Existe plano de continuidade de negócios?**
   Não. O PCN será documento acessório da PSI. Porém, há ações desenvolvidas para garantia de continuidade em caso de desastres, como ambiente de backup e guarda externa de dados.

3. **É realizada a classificação da informação (exemplo: confidencial, restrita, interna, pública)?**
   Não.

4. **Existe analise de risco pela área de TI?**
   Não formalmente, mas há análise dos riscos externos em relação ao ambiente externo, como parte das atividades rotineiras da COTEC.

5. **Existe comitê que decida sobre a priorização das ações e investimentos de TI?**
   Existiu um comitê responsável pela elaboração do PDTI 2015/2016, que executou essa função.

6. **É realizada a gestão dos níveis de serviço acordados para os serviços de TI?**
   Não formalmente. A Carta de Acordo de Níveis de Serviço da Funpresp-Jud está prevista no PDTI para ser entregue até agosto de 2016.

7. **Em relação ao PDTI – Plano Diretor de Tecnologia da Informação:**
   a) foram vinculados indicadores e metas para cada ação? Sim.
   b) os custos estão vinculados às atividades e projetos de TI? Sim.
   c) foi realizado inventário de todos os ativos de TI? Sim.

8. **Existe um processo de aferição de conformidade às normas de segurança da informação?**
   Não.

9. **Existe a determinação dos responsáveis pela segurança das informações da Entidade?**
   Não existe uma determinação formal, mas a COTEC efetua a gestão da segurança.

Controle de acessos

10. **Existe processo formalizado com as responsabilidades do processo de concessão, alteração e remoção de acesso físico e lógico aos usuários internos e externos?**
    Não, mas, em função do tamanho da Fundação, periodicamente, são revisados cadastros e privilégios concedidos, havendo logs dos acessos efetuados.

11. **São exigidos níveis de segurança mínimos para elaboração das senhas?**
    Sim.

12. **As senhas são atualizadas periodicamente?**
    Não.

13. **São revistos periodicamente quais usuários possuem acesso aos diretórios e sistemas utilizados pelas áreas?**
    Sim, mas sem um processo formal.

14. **Existe procedimento para liberação de acesso remoto? Os usuários que possuem acesso remoto estão sujeitos à autenticação?**
    Não, mas todo usuário externo está sujeito à autenticação, além de ser utilizada VPN criptografada para o acesso.

Gestão de incidentes de segurança da informação

15. **Existem procedimentos e responsabilidades definidas para incidentes de segurança?**
Não.

16. **Existem procedimentos e responsabilidades definidas do reporte de incidentes de segurança relacionados com serviços terceirizados?**
Não.

17. **Existe segregação de ambientes de desenvolvimento, homologação e produção dos sistemas utilizados pela Funpresp-Jud?**
Sim, a Fundação possui os três ambientes para seus sistemas.

Gestão de contratos

18. **É adotado processo de trabalho formal na gestão de contratos de bens e serviços de TI?**
Não.

19. **Em relação à gestão de contratos, de quem é a responsabilidade por:**

a) Monitorar a execução contratual do ponto de vista de resultados de negócio? COTEC
b) Monitorar a execução técnica dos serviços contratados? COTEC
c) Gerir o contrato com base em resultados? COTEC
d) Acompanhar e fiscalizar o contrato? COTEC

20. **Nos contratos são estabelecidas normas de segurança da informação?**
Parcialmente.

Armazenamento e cópias de segurança dos dados (*backups*)

21. **Os procedimentos adotados para realização e recuperação das cópias de segurança dos dados estão formalizados?**
Não. Porém existe política de backup informal com retenções definidas e escopo bem delimitado.

22. **A frequência com que as cópias de segurança devem ser realizadas está estabelecida de acordo com a criticidade da informação?**
Parcialmente.

23. **As cópias de segurança são mantidas em local remoto para livrá-las de qualquer dano que possa ocorrer na instalação principal?**
Sim.

24. **Todas as cópias de segurança são devidamente documentadas em relação à data da execução e o seu conteúdo?**
Sim.

25. **As cópias possuem um nível adequado de segurança física e ambiental, utilizando os mesmos padrões da instalação principal?**
Não. Porém há previsão de que até dezembro de 2015 tenhamos o requisito atendido.

26. **É executado um nível mínimo de cópias de segurança dos dados e de softwares essenciais para a Funpresp-Jud?**
Sim.

Segurança / Antivírus

27. **Existem procedimentos para identificação de softwares maliciosos (antivírus)?**
Sim.

28. **Os procedimentos de atualização do antivírus nas estações de trabalho são automáticos?**
Sim.

29. **Quando é identificado um software malicioso (vírus), há procedimentos de análise e correção?**
Sim.

30. **Os computadores móveis são protegidos com travas de segurança?**
Do ponto de vista lógico, sim. Porém não há criptografia de dados, apenas controle de acesso, uma vez que as informações sensíveis da Fundação ficam armazenadas na rede, e a utilização de computadores móveis hoje se restringe a apresentações institucionais, que são públicas.

3. DA ANÁLISE

O controle das atividades da área de Tecnologia e Informação tem o objetivo de verificar a confidencialidade, disponibilidade e a integridade das informações.

Percebe-se a evolução da área de Tecnologia da Informação com relação às questões estruturais, destacando-se como positivo o desenvolvimento do Plano Diretor de Tecnologia da Informação – PDTI, aprovado pelo Conselho Deliberativo em 03 de setembro de 2015. O escopo do documento abrangeu todas as ações e projetos compreendidos no biênio 2015-2016 e o trabalho foi desenvolvido por um comitê específico, que propôs, também, a priorização das ações e investimentos de TI.

Neste momento de funcionamento da Fundação é essencial buscar a implementação e a padronização dos seus procedimentos internos, sendo fundamental concentrar esforços na execução das ações e projetos previstos.

Nesse contexto, é importante citar a edição da Orientação Interna PRESI/GABIN nº 04, de 23 de setembro de 2015, que dispõe sobre procedimentos operacionais e fluxo de demandas referentes à tecnologia da informação.

É relevante que se realize a **modelagem/mapeamento de processos** da área de Tecnologia e Informação, alinhados com a estratégia, os objetivos e as ações da organização, objetivando eficiência e uma melhoria contínua dos processos.

O mapeamento de processos e a manualização de procedimentos são ferramentas importantes de controle e contribuem para eficiência e uma melhoria contínua dos processos.

É relevante que o mapeamento se insira em um ciclo maior de mapeamento das demais unidades, processos, riscos e controles de toda a Fundação. Isso contribui para uma maior integração entre as áreas técnicas envolvidas, especialmente entre a contábil, a financeira, a de arrecadação e a de investimentos, visando a otimização e segurança nos processos de trabalho.

4. PLANO DE RECOMENDAÇÕES

É importante que cada área estruture seus controles internos próprios a serem aplicados no desempenho das atividades, seja por meio da adoção de rotinas, sistemas, relatórios ou procedimentos de verificação, remetendo os resultados alcançados às instâncias de supervisão.

Neste contexto, recomenda-se:

i. implementar e padronizar os procedimentos internos, sendo fundamental concentrar esforços na execução das ações e projetos previstos no PDTI.

ii. realizar a modelagem/mapeamento de processos da área de Tecnologia e Informação, alinhados com a estratégia, com os objetivos e com as ações da Fundação, objetivando eficiência e uma melhoria contínua dos processos;

iii. elaborar e publicar política de segurança da informação que contemple o plano de continuidade de negócios e a designação formal dos responsáveis pela segurança das informações da Fundação;

iv. formalizar o processo de concessão, alteração e remoção de acesso físico e lógico aos usuários internos e externos;

v. formalizar o procedimento e responsabilidades definidas para incidentes de segurança da informação, inclusive relacionado com os serviços terceirizados;

vi. formalizar os procedimentos adotados para realização e recuperação das cópias de backup contendo a definição da frequência com que as cópias devem ser realizadas;

vii. envidar esforços para cumprimento do prazo para definição de acordos de níveis de serviço (SLA);

viii. executar as ações necessárias ao cumprimento dos procedimentos operacionais e fluxo de demandas referentes à tecnologia da informação de acordo com a Orientação Interna PRESI/GABIN nº 04, de 23 de setembro 2015.

Por fim, como boa prática gerencial recomenda-se a emissão de relatórios de atividades que descrevam com tempestividade e adequação as principais ações desempenhadas, os controles internos aplicados pela própria unidade e o acompanhamento dos indicadores da área, sendo recomendável a apresentação dos resultados aos órgãos estatutários e de controle competentes.

5. ENCAMINHAMENTO

Apresentadas as informações e o plano de recomendações sobre os procedimentos de armazenamento e segurança de dados, sugere-se o encaminhamento do presente Relatório à Diretora-Presidente e na sequência à Diretoria Executiva para apreciação, recomendando-se posterior encaminhamento aos Conselhos Fiscal e Deliberativo.

Brasília, 07 de dezembro de 2015.

Fabíola S. Carvalhedo

Fabíola Silva Carvalhedo
Assessora de Controle Interno

1. Ciente.
2. Encaminhe-se o presente Relatório para conhecimento e apreciação da Diretoria Executiva, e posterior envio aos Conselhos Deliberativo e Fiscal.

Elaine de Oliveira Castro

ELAINE DE OLIVEIRA CASTRO
Diretora-Presidente