NUCLEO CONSULTORIA EM SEGURANÇA

Artigo

SPED – Sistema Público de Escrituração Fiscal
CONTROLES MÍNIMOS PARA A SEGURANÇA DA INFORMAÇÃO

Prof. Ms. Edison Fontes, CISM, CISA, CRISC

BRASIL, São Paulo

Novembro, 2013

V.1.0

1. RESUMO

Este artigo apresenta os controles mínimos de segurança da informação que são necessários para a organização utilizar o SPED – Sistema Público de Escrituração Fiscal no Brasil.

A Norma NBR 27002 ISO/IEC 27002:2005 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação, ABNT, define 133 (cento e trinta e três) controles de segurança da informação. **Porém, quais seriam os controles de segurança da informação prioritários para uma organização que está implantando o SPED?** Esta resposta é dada pelo autor, considerando as principais características do Serviço SPED, a sua experiência em gestão da segurança da informação e os seus estudos acadêmicos como pesquisador e professor.

A não implementação destes controles mínimos coloca a organização em risco. Ela estará utilizando a tecnologia do Documento Eletrônico sem uma base estruturada de proteção da informação e consequentemente poderá ser impactada pela indisponibilidade do sistema SPED, por não possibilidade de cumprimento de prazos, por erros, por fraude, por vazamento de informação e pelo não cumprimento de legislações que exigem das organizações:

- *a existência de mecanismos de segurança (Lei 12.737/2012),*
- *cuidado e diligência do gestor organizacional (Artigo 1011-CC),*
- *privacidade, confidencialidade e segurança (Decreto 7.963/13),*
- *melhores práticas de segurança da informação (Lei 12.413/2013).*

A elaboração deste artigo foi motivada pelo fato de que (normalmente) quando se trata do Serviço SPED, a preocupação é exclusiva com as regras do mesmo e como este novo sistema impactará a organização. Pouco se fala sobre os controles de segurança da informação que devem existir. Este artigo é uma contribuição para todos aqueles que estão direta ou indiretamente relacionados ao Sistema SPED. Desejo a todos os leitores, que este artigo lhe traga proveito no que diz à segurança da informação para o uso do SPED.

Críticas e observações podem e devem ser enviadas ao autor para a melhoria do texto e melhoria do compartilhamento de conhecimento.

Um grande abraço
Edison Fontes, CISM, CISA, CRISC
edison@pobox.com
www.nucleoconsult.com.br

2. CARACTERÍSTICAS DO SPED EM RELAÇÃO À INFORMAÇÂO

O SPED trouxe para a organização, de maneira completa e obrigatória, o uso da informação digital (representação da informação em sinais eletrônicos chamados de bits e bytes), encerrando o ciclo de reinado da informação em papel (meio físico formado por átomos, se confunde com a própria informação). É um novo, desafiante e obrigatório momento para a organização.

O SPED possui algumas características principais que relacionamos abaixo:

2.1. Uso do documento eletrônico.

=> O SPED inaugura formalmente, ou digamos obriga formalmente, a utilização do documento eletrônico. O documento em papel deixa de existir como um documento. Pode existir como uma cópia que facilita a leitura dos usuários.

2.2. Autenticação do documento pelo usuário

=> De maneira similar ao documento em papel, o documento eletrônico também precisa ser assinado por um usuário, ou mais de um usuário, para legalizar a responsabilidade de quem confirma aquele documento.

2.3. Autenticação utilizando o Certificado Digital

=> Em um documento eletrônico a assinatura é realizada utilizando um Certificado Digital que contém dados de um usuário. É de uso individual.

2.4. Guarda de documento eletrônico.

=> Mesmo com as informações no formato digital, continua existindo a necessidade de guarda de documentos. Neste caso, de documentos eletrônicos, inclusive cópias que permitam manter a existência dos documentos eletrônicos caso o arquivo principal seja destruído ou corrompido.

2.5.Transmissão de documento eletrônico.

=> Da mesma maneira que documentos em papel eram entregues fisicamente para os órgãos do governo, documentos eletrônicos precisam ser enviados de maneira digital para os mesmos órgãos do governo.

2.6. Autorização para a realização da transmissão.

=> Para qualquer ação no uso do SPED, a realização da transmissão exige uma autorização para que a mesma seja realizada. Citamos o exemplo da transmissão, pois qualquer erro no envio de informações para o governo, uma transmissão realizada se for com erros, gerará retrabalho e trará impactos.

2. 7. Existência de Cópias de Segurança.

=> De maneira idêntica à informação no papel, a informação digital precisa ter cópias de segurança para garantir que mesmos que as informações principais sejam destruídas (erro, desastre ou fraudes), existem cópias de segurança que permitirá a organização a refazer o ambiente da informação.

Prof. Ms. Edison Fontes, CISM, CISA, CRISC – edison@pobox.com - www.nucleoconsult.com.br

2.8. Troca de informações
=> O documento eletrônico será enviado para o governo e eventualmente para outros órgãos, e é necessário que esta informação esteja integra, não corrompida. Caso contrário a organização será responsabilizada.

2. 9. Rigoroso cronograma de atividades.
=> O relacionamento de envio de documentos para o governo exige o cumprimento de uma agenda apertada e que qualquer erro ou atraso pode comprometer a situação de organização em relação ao governo.

2.10. Organização não tem escolha.
=> O SPED, e outras ações do governo digital não tem retorno. Pode-se discutir o quando acontecerá. Mas, acontecerá. E desta maneira a organização precisa estar preparada para o ambiente digital, o documento eletrônico e a pessoa humana ainda não digital. Todas as ações acima detalhadas são comandadas (ainda) pelos humanos.

3. CONTROLES PARA A SEGURANÇA DA INFORMAÇÂO

A Norma NBR ISO/IEC 27002:2005 é a norma estrutural da Família de Normas ISO/IEC 27000 e será com ela que embasaremos nossas recomendações.

Esta norma possui 133 (cento e trinta e três) controles para um Processo Organizacional para a Segurança da Informação, os quais agrupamos em 14 Dimensões apresentadas na Figura 1 abaixo.

Figura 1: DIMENSÔES DA SEGURANÇA DA INFORMAÇÃO
Fonte: Livro Praticando a segurança da informação, Edison Fontes, Editora BRASPORT, 2008.
Estrutura baseada na Norma Internacional ISO/IEC 27002:2005

Indicamos a seguir os controles mínimos que uma organização deve implementar para quando do uso do Sistema SPED.

3.1 – Políticas e normas de segurança da informação
=> Devem existir regulamentos indicando as responsabilidades e o padrão de rigidez dos controles de segurança da informação. É obrigatório que estes regulamentos sejam de conhecimento de todos e sejam cumpridos por todos os funcionários, prestadores de serviço, estagiários e outros tipos de usuários do ambiente computacional.
=> Este conjunto de regulamentos pode variar de um único documento (para pequenas organizações) até um conjunto de dez a quinze documentos para médias e grandes organizações.

3.2 – Gestor da Segurança da Informação
=> Deve-se nomear um Gestor da Segurança da Informação que terá a responsabilidade de desenvolver e implantar o Processo Organizacional de Segurança da Informação.
=> Para organizações menores, este Gestor da Segurança da Informação pode ser um consultor ou um funcionário em período parcial.

3.3 – Identificação e autenticação dos usuários
=> Quando da comunicação com o Sistema SPED do governo, a identificação e autenticação do usuário ou da organização acontecerá utilizando o Certificado Digital. Porém, internamente, no Sistema SPED da organização, deve-se definir como será a identificação e autenticação do usuário, de maneira a garantir a individualidade dos acessos e o segredo da autenticação.
=> Deve existir um controle das identificações dos usuários.

3.4 – Garantia de usuários válidos
=> Deve existir um rigoroso controle para que apenas os usuários válidos estejam cadastrados no sistema. Isto significa que quando um funcionário ou prestador de serviço deixar a organização, sua identificação imediatamente deve ser bloqueada, impedindo o seu uso por esta pessoa ou o uso fraudulento desta identificação por outra pessoa.

3.5 – Uso do Certificado Digital
=> O uso do Certificado Digital acarreta um excelente padrão de segurança para a identificação e autenticação do usuário. Porém é obrigatório a organização planejar soluções para as seguintes situações:

a) Encerramento do prazo de validade do certificado.
b) Perda do certificado.
c) Roubo do certificado.
d) Destruição involuntária do certificado.
e) Esquecimento da senha do certificado.
f) Ausência da pessoa que possui o certificado.

3.6 – Autorizador do uso da informação (Gestor da Informação)

=> Toda transação do sistema SPED ou de outro sistema, deve ter sua autorização para que um usuário a utilize. Desta maneira a organização precisa ter um Gestor para cada informação. Em uma organização pequena provavelmente será o proprietário da organização.

=> Este Gestor da Informação deverá definir/autorizar:

a) Os usuários que podem ter acesso a informação.
b) O tempo de guarda desta informação.
c) O tempo que será exigido para uma situação de recuperação de uma indisponibilidade.
d) A necessidade (considerando os aspectos legais e operacionais) da necessidade de existência e guarda dos registros das operações realizadas (log de auditoria).

3.7 – Plano para situações de contingência

=> É obrigatório a organização ter um plano para situações de contingencia, quando por algum motivo o sistema SPED ou os recursos que possibilitam o uso do Sistema SPED estejam indisponíveis.

=> Deve-se considerar a indisponibilidade de:

a) Sistema aplicativo.
b) Linhas de comunicação.
c) Certificados digitais.
d) Pessoas conhecedoras dos procedimentos.
e) Ambiente computacional.
f) Ambiente do escritório onde as pessoas trabalham.

3.8 – Documentação para o funcionamento do ambiente SPED

=> Deve existir uma documentação que registre como as atividades relacionadas ao SPED devem ser executadas, permitindo que outras pessoas com o mesmo perfil profissional da pessoa primária responsável, possam executar estas tarefas, mesmo com um pouco mais de tempo. Porém, sem deixar que a organização realize seus compromissos em relação ao SPED.

3.9 – Guarda de documentos

=> É necessário a a existência de cópias de informações. Estas cópias precisam ter uma duplicidade (cópias de segurança) e todas elas devem ser guardadas em local seguro. As cópias de segurança devem ser guardadas em local alternativo distante o suficiente para estar segura caso exista uma situação de destruição ou indisponibilidade das cópias e informações originais.

=> Estas copias precisam ser validadas periodicamente.

=> Estas cópias precisam considerar que ao longo do tempo a mídia de armazenamento pode ficar obsoleta.

3.10 – Treinamento das Pessoas

=> Todos os usuários precisam ser conscientizados e treinados em relação à segurança da informação.

=> Cada usuário precisa saber as suas responsabilidades e deve formalizar este conhecimento em um termo indicando seu conhecimento em relação às regras e regulamentos da organização.

3.11 – Gestão de riscos

=> Deve-se realizar periodicamente, no mínimo a cada doze meses, uma avaliação dos riscos, considerando a informação e os controles de proteção da informação.
=> Esta avaliação gerará ações para novos controles ou aprimoramento dos controles de segurança da informação existentes.

3.12 – Procedimentos Formalizados

=> O SPED exige datas rígidas e obrigatórias para várias ações. Deve existir um controle formal, estruturado e atualizado para garantir o cumprimento destas obrigações operacionais. Este controle deve ser revisado periodicamente e avaliado se está atendendo as necessidades da organização.

4. CONCLUSÃO

O SPED é o grande sistema que está realizando uma transformação no ambiente da informação da organização. O Documento Eletrônico é uma realidade, uma obrigação e um elemento que necessita de segurança.

Os controles aqui detalhados são os elementos mínimos que que devem constar no Plano Organizacional de Segurança da Informação. Independente do seu porte, a organização tem condições de ter este processo de segurança.

Evidentemente após a implantação destes controles mínimos, a organização deve contemplar os demais controles e deve estruturar o seu Processo Organizacional de Segurança da Informação, considerando o seu porte, seu tipo de atividade e seus objetivos organizacionais.

É um caminho longo, mas um caminho possível e que deve ser feito de maneira profissional. Caso contrário, o caos é certo!

Grande abraço,

Prof. Ms. Edison Fontes, CISM, CISA, CRISC
Consultor em Segurança da Informação, Gestão de Risco, Continuidade de Negócio, Conscientização de Pessoas.
edison@pobox.com
www.nucleoconsult.com.br
@edisonfontes

Livros do Autor:
- Políticas e normas para a segurança da informação, *Editora Brasport, 2012.*
- Clicando com segurança, *Editora Brasport, 2011.*
- Praticando a segurança da informação, *Editora Brasport, 2008.*
- Segurança da informação: o usuário faz a diferença, *Editora Saraiva, 2006.*
- Vivendo a segurança da informação, *Editora Sicurezza, 2000. Esgotado.*