MANUAL DE GOVERNANÇA EM SEGURANÇA DA INFORMAÇÃO

ABRAPP

MANUAL DE GOVERNANÇA EM SEGURANÇA DA INFORMAÇÃO

Comissão Técnica Nacional
de Governança

novembro/2014

ABRAPP

SUMÁRIO

APRESENTAÇÃO

A Abrapp tem a satisfação de apresentar às suas associadas o **Manual de Governança em Segurança da Informação**, idealizado e coordenado pela Comissão Técnica Nacional de Governança.

A Comissão Técnica Nacional de Governança surgiu em Julho de 2007, fruto da união de esforços da Comissão de Controles Internos e *Compliance* e da Comissão de Gestão Corporativa.

Desde então, a Comissão Técnica Nacional de Governança e as Comissões Técnicas Regionais de Governança têm se dedicado à análise, estudo e debate dos temas que envolvem principalmente as questões da governança das EFPC, de modo a oferecer às associadas da Abrapp uma interpretação adequada e privilegiada desse importante assunto.

Essa interpretação não se caracteriza apenas com a disponibilização de produtos pela Abrapp - por exemplo, planilhas de autoavaliação, calendário automatizado de obrigações legais - mas também com a oferta de literatura de qualidade como o Manual de Controles Internos, o Guia de Boas Práticas para Planos de Continuidade de Negócios e o Livro Gestão Baseada em Riscos, entre outros, sem contar os eventos dos quais a Comissão Nacional e as Comissões Regionais de Governança tomam parte (Congressos e Encontros).

Nesse sentido, a Comissão Técnica Nacional de Governança produziu o presente Manual, com o intuito de destacar as questões relevantes envolvendo a Segurança da Informação, que com o advento de novas formas e veículos de comunicação trazidas pela incrível evolução tecnológica, deixa de ser apenas uma preocupação das áreas de Tecnologia da Informação das empresas e passa a ser uma preocupação corporativa.

Paralelamente, o papel das EFPC como agentes fiduciários de valores e informações de participantes e assistidos e a existência da garantia constitucional dos princípios de sigilo e inviolabilidade das informações faz com que essa preocupação seja prioridade no âmbito dos riscos operacionais e estratégicos das entidades.

Assim, este trabalho pretende fornecer diretrizes, conceitos e orientações básicas às EFPC na definição e implantação de uma política robusta de Segurança da Informação, contudo este Manual é simplesmente o ponto de partida de um processo que deve ser continuamente avaliado e aperfeiçoado.

SUMÁRIO EXECUTIVO

Os capítulos iniciais do Manual de Governança em Segurança da Informação - 2 ao 5 - tratam de apresentar os conceitos fundamentais de itens que serão desenvolvidos ao longo do documento.

Nos capítulos 6, 7 e 8 o conteúdo exposto tem grande validade prática, visto que os procedimentos e boas práticas são detalhados, com a citação das diversas metodologias para abordar o tema.

Os capítulos 9 e 10 dão destaque à questão da formalização, ou seja, a implantação de programa e política da segurança da informação.

Nos capítulos 11, 12 e 13 as questões específicas da informação - classificação, levantamento e tratamento são abordadas.

O capítulo 14 trata do Plano de Continuidade de Negócios - PCN, ao passo que o capítulo 15 traz possíveis testes de verificação que podem ser aplicados.

Nos capítulos 16, 17 e 18 são abordados a questão da "transparência x segurança", o entendimento do assunto pelas empresas e quais são os riscos inerentes.

Por fim, nos capítulos finais 19, 20 e 21 são tratados assuntos emergentes como Gerenciamento Eletrônico de Documentos - GED, informação na "nuvem" e a comunicação notadamente em tempos das redes sociais.

1. INTRODUÇÃO

A Resolução CGPC nº 13/2004, que estabelece princípios, regras e práticas de governança, gestão e controles internos a serem observados pelas Entidades Fechadas de Previdência Complementar – EFPC, em seu artigo 18 preconiza que os sistemas de informações, inclusive gerenciais, devem ser confiáveis e abranger todas as atividades das EFPC. Já o parágrafo primeiro estabelece a necessidade de se prever procedimentos de contingência e segregação de funções entre usuários e administradores dos sistemas informatizados, de forma a garantir a integridade e segurança, inclusive dos dados armazenados.

No âmbito do sistema fechado de previdência complementar a "informação" tem um valor essencial, tido como um direito fundamental dos participantes e assistidos e, nesses termos, sendo a segurança de dados e informações responsabilidade de todos, é preciso definir um padrão mínimo de condutas a ser seguido, atribuindo maior confiabilidade aos processos internos.

Para que a informação seja confiável e íntegra, é essencial que as EFPC estabeleçam suas diretrizes de segurança, definindo com clareza a filosofia da organização em relação ao uso e proteção da informação. Também é de suma importância definir a unidade da entidade que se responsabilizará pela coordenação do processo de segurança da informação e estabelecer norma interna que especifique a forma de atuação dos agentes nas diversas etapas do processo.

Nesse contexto, o presente Manual de Governança em Segurança da Informação objetiva auxiliar as EFPC no estabelecimento das normas básicas para o processamento, classificação, reclassificação, transmissão, armazenamento e destruição das informações de acordo com o grau de sigilo, independentemente do suporte ou forma em que a informação seja armazenada, veiculada ou transportada.

É importante que todos os profissionais, de todos os níveis, tenham a consciência de que o tempo todo manuseamos dados e geramos informações que tramitam em sistemas, em meios físicos, na forma escrita e verbal e em uma velocidade cada vez maior por conta dos meios de comunicação existentes e de sua constante evolução.

Tal velocidade se por um lado pode trazer benefícios, por outro nos deixa expostos a riscos de diversas naturezas uma vez que estas informações podem ser perdidas, utilizadas de forma inadequada ou mesmo alteradas in-

devidamente. E, pensando que a materialização destes riscos pode comprometer os objetivos das Entidades Fechadas de Previdência Complementar, a Comissão Técnica Nacional de Governança coordenou com suas Comissões Regionais Centro Norte e Sul, a elaboração deste material que, de alguma forma, espera-se que possa contribuir para melhoria da gestão da segurança da informação das EFPC.

Esclarece-se, por fim, que este material não substitui o "Manual de Boas Práticas em Tecnologia da Informação", editado pela Comissão Técnica Nacional de Tecnologia da Informação da Abrapp, cujo enfoque é direcionado à TI - Tecnologia da Informação em seu aspecto mais abrangente.

2. O QUE É INFORMAÇÃO

Informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação quantitativa ou qualitativa no conhecimento do receptor (Fonte: Wikipédia).

A Informação carrega uma diversidade de significados e, genericamente, o conceito de informação está ligado às noções de restrição, comunicação, controle, dados, forma, instrução, conhecimento, significado, estímulo, padrão, percepção e representação de conhecimento.

A Informação é um ativo que, como qualquer outro ativo importante é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Como resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (ABNT NBR ISO/IEC 17799:2005).

3. O QUE É SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação refere-se à proteção existente sobre as informações de uma determinada organização ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais, de modo a garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pelas entidades; adicionalmente, outras propriedades tais como, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição (Fonte: Wikipédia).

A segurança da informação é um conjunto de medidas com objetivo de proteger as informações detidas pelas EFPC a fim de garantir a continuidade do negócio e minimizar os riscos de utilização por pessoas não autorizadas.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessário, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos (ISO 17799 2005, p X).

No que se refere à segurança da Informação sugere-se que sejam estabelecidas, no mínimo, as seguintes regras:

a) Padrões de utilização de criptografia;

b) Normas para utilização do e-mail, controle de acesso à Internet, recursos e sistemas computacionais;

c) Normas para utilização de programas e equipamentos;

d) Procedimentos para guarda adequada das informações e back-up;

e) Procedimentos para utilização de mídias removíveis;

f) Definição de responsabilidades e perímetros de segurança;

g) Plano de Contingência;

h) Segurança lógica (políticas de senha, sistemas de autenticação de

usuário, programa de detecção de vírus);

i) Segurança física (acesso de empregados e prestadores de serviço), guarda e proteção de equipamentos, condição das instalações elétricas, climatização dos ambientes, dentre outros.

j) Normas sobre a propriedade de programas desenvolvidos por empregados;

k) Normas para comunicação de incidentes;

l) Regras sobre o monitoramento das informações no ambiente corporativo;

m) Normas para análise e gerência de riscos sobre segurança da informação;

n) Classificação das informações quanto ao seu uso (pública, corporativa, interna, restrita, confidencial);

o) Normas de consequências de violação da segurança da informação; e

p) Plano de comunicação, treinamento e conscientização sobre segurança da informação.

4. IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

O valor da informação não é facilmente mensurável principalmente porque as ameaças que podem afetá-la, causando prejuízos às atividades das EFPC, estão em todo lugar.

Por essa razão a segurança da informação precisa ser tratada de forma abrangente, por ser algo que diz respeito à toda a corporação, em todas as áreas e processos, não restritivamente à tecnologia da informação.

É responsabilidade das EFPC zelar pela segurança, integridade e confiabilidade das informações, especialmente para assegurar o pleno atendimento de suas finalidades.

Em nosso sistema legal, essa responsabilidade emana do §1º do Artigo 202 da Constituição Federal, e vem tratada nas Leis Complementares nºs 108 e 109/2001, e em vários normativos expedidos pelos órgãos de regulação e de supervisão/fiscalização das EFPC:

> A ação do Estado é exercida com o objetivo de, dentre outros, assegurar aos participantes e assistidos o pleno acesso às informações relativas à gestão de seus respectivos planos de benefícios. (artigo 3º, IV da Lei Complementar nº 109/2001)
>
> A divulgação aos participantes, inclusive aos assistidos, das informações pertinentes aos planos de benefícios dar-se-á ao menos uma vez ao ano . (artigo 24 da Lei Complementar nº 109/2001)
>
> As informações requeridas formalmente pelo participante ou assistido, para defesa de direitos e esclarecimento de situações de interesse pessoal específico deverão ser atendidas pela entidade no prazo estabelecido pelo órgão regulador e fiscalizador. (§único do artigo 24 da da Lei Complementar nº 109/2001)
>
> A fiscalização das entidades de previdência complementar terá livre acesso às respectivas entidades, delas podendo requisitar e apreender livros, notas técnicas e quaisquer documentos, caracterizando-se embaraço à fiscalização, sujeito às penalidades previstas em lei, qualquer dificuldade oposta à consecução desse objetivo. (artigo 41 da Lei Complementar nº 109/2001)
>
> O órgão regulador e fiscalizador das entidades fechadas poderá solicitar dos patrocinadores e instituidores informações relativas aos aspectos específicos que digam respeito aos compromissos assumidos frente aos respectivos planos de benefícios. (§1º do artigo 41 da Lei Complementar nº 109/2001)

Os sistemas de informações, inclusive gerenciais, devem ser confiáveis e abranger todas as atividades da EFPC. (artigo 18 da Resolução CGPC nº 13/2004)

Os órgãos de governança e gestão da EFPC devem zelar permanentemente pela exatidão e consistência das informações cadastrais. (§ 2º do artigo 18 da Resolução CGPC nº 13/2004)

A comunicação com os participantes e assistidos deve ser em linguagem clara e acessível, utilizando-se de meios apropriados com informações circunstanciadas sobre a saúde financeira e atuarial do plano, os custos incorridos e os objetivos traçados, bem como, sempre que solicitado pelos interessados, sobre a situação individual perante o plano de benefícios de que participam. (artigo 17 da Resolução CGPC nº 13/2004)

A estrutura organizacional deve permitir o fluxo de informações entre os vários níveis de gestão e adequado nível de supervisão. (artigo 7º da Resolução CGPC nº 13/2004)

Na divulgação de informações aos participantes e assistidos de planos de caráter previdenciário que administram as EFPC deverão observar o disposto em norma do órgão regulador e de supervisão. (Resolução MPAS/CGPC nº 23/2006 e legislação correlata, Instrução Previc nº 11/2014)

A EFPC deverá manter sua própria base de dados cadastrais de forma atualizada, confiável, segura e segregada por plano de benefícios, independentemente da obrigatoriedade de envio de dados à PREVIC. (artigo 6º da Instrução SPC nº 23/2008)

Todas as informações enviadas à PREVIC, por meio do SICADI, são de inteira responsabilidade da EFPC, que responderá por erros ou omissões nela presentes. (artigo 21 da Instrução PREVIC nº 02/2010)

Infrações e Penalidades aplicáveis em:

Deixar de divulgar aos participantes e aos assistidos, na forma, no prazo ou pelos meios determinados pelo Conselho de Gestão da Previdência Complementar e pela Secretaria de Previdência Complementar, ou pelo Conselho Monetário Nacional, informações contábeis, atuariais, financeiras ou de investimentos relativas ao plano de benefícios ao qual estejam vinculados. (artigo 81 do Decreto nº 4.942/2003 - DOU de 31/12/2003)

Deixar de prestar à Secretaria de Previdência Complementar informações contábeis, atuariais, financeiras, de investimentos ou outras previstas na regulamentação, relativamente ao plano de benefícios e à própria entidade fechada de previdência complementar, no prazo e na forma determinados pelo Conselho de Gestão da Previdência Complementar e pela Secretaria de

Previdência Complementar. (artigo 82 do decreto nº 4.942/2003 - DOU de 31/12/2003)

Deixar de prestar ou prestar fora do prazo ou de forma inadequada informações ou esclarecimentos específicos solicitados formalmente pela Secretaria de Previdência Complementar. (artigo 95 do Decreto nº 4.942/2003 - DOU de 31/12/2003)

Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas.

5. RISCOS DE SEGURANÇA DA INFORMAÇÃO

Riscos de segurança da informação são as possibilidades de uma ameaça explorar vulnerabilidades dos ativos, comprometendo a confidencialidade, integridade, autenticidade e disponibilidade das informações da entidade.

Cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança. Desta forma, conclui-se que são as vulnerabilidades as principais causas das ocorrências de incidentes de segurança.

A vulnerabilidade é um ponto fraco que permite a ação indevida de agentes. A ameaça é o agente que se aproveita da vulnerabilidade para atingir seu intento. Quando existem a vulnerabilidade e a ameaça simultaneamente, ocorre o RISCO. Por exemplo:

> Seu computador não tem antivírus, sendo esta uma vulnerabilidade. Você pode receber e-mail com vírus sendo esta uma ameaça que se aproveita da vulnerabilidade de não ter o antivírus. O RISCO é o produto da vulnerabilidade *versus* ameaça.

As ameaças podem partir de dentro ou de fora das EFPC, alguns exemplos são: acesso indevido, roubo de informação, engenharia social, espionagem industrial, fraudes, erros, acidentes e catástrofe naturais, podendo gerar altos prejuízo e até interrupção total das atividades da entidade dependendo do impacto no negócio.

Portanto, não sendo possível eliminar todas as ameaças, então, deve-se partir para mitigação dos riscos a que a EFPC esteja exposta, no exemplo citado, mediante a redução das vulnerabilidades, ou seja, por meio da instalação de um antivírus e/ou diminuindo as ameaças, seguindo regras de segurança, lembrando que muitas vezes a ameaça é física e decorre de desvios de conduta dos sujeitos que manipulam a informação.

A seguir, demonstra-se o fluxo de evento de vulnerabilidade de um ponto fraco:

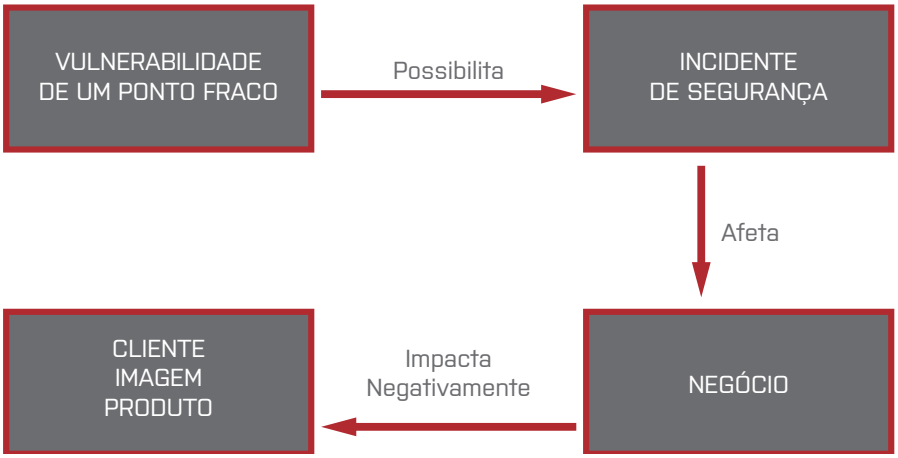


Figura 1

Os ativos devem ser protegidos contra as ameaças de todos os tipos, a fim de garantir os quatro princípios básicos da segurança da informação:

Confidencialidade: as informações devem ser conhecidas apenas pelos indivíduos que detém as permissões de acesso, evitando assim o vazamento de informação.

Integridade: as informações devem ser mantidas no seu estado original, sem alterações, garantindo a quem as receber, a certeza de que não foram falsificadas ou alteradas.

Autenticidade: garantia da veracidade da fonte das informações. Esta pode ser obtida por meio da autenticação, onde é possível confirmar a identidade da pessoa ou entidade que presta as informações.

Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (ISO 17799).

Abaixo relaciona-se as principais ameaças que podem impactar no bom desempenho do processo de segurança da informação nas EFPC:

a) Vírus;

b) Funcionários insatisfeitos;

c) Divulgações de senhas;

d) Acessos indevidos;

e) Vazamento de informações;

f) Fraudes, erros e acidentes;

g) *Hackers* (perigosa combinação de conhecimento de TI com motivação);

h) Falhas na segurança física;

i) Uso de notebooks e mídias removíveis;

j) Fraudes em e-mail;

k) Perda/extravio de documentos;

l) Ações de engenharia social (prática de interações humanas para que pessoas violem os procedimentos de segurança da informação).

Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um Sistema de Gestão da Segurança da Informação - SGSI (ISO 27005, 2008, p3).

6. ADOÇÃO DE BOAS PRÁTICAS DE SEGURANÇA DE INFORMAÇÃO É UMA INICIATIVA DE TODA CORPORAÇÃO

Para implantação bem sucedida da segurança da informação, alguns procedimentos devem ser vistos com atenção. Dentre normas e melhores práticas adotadas no mundo todo seguem alguns exemplos que não estão restritos à tecnologia da informação, mas que são de extrema importância em qualquer processo de implantação dessa iniciativa.

A. Segurança na contratação de pessoas

Política de segurança ao contratar pessoas. Os funcionários devem assinar termos de confidencialidade. Definições de condições de trabalho devem especificar as responsabilidades dos funcionários quanto à segurança da informação.

B. Treinamento dos usuários

Educação, conscientização e treinamento referentes à segurança da informação. De que adianta ter uma estrutura de controle eficaz se algum funcionário conversar sobre algum assunto sigiloso da empresa em local público (essência da engenharia social[1]).

Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamentos apropriados para conscientização e atualizações regulares nas políticas e procedimentos organizacionais relevantes para as suas funções.

O treinamento para aumentar a conscientização visa permitir que as pessoas reconheçam os problemas e incidentes de segurança da informação e respondam de acordo com as necessidades do seu trabalho. (ISO 17799)

C. Segurança física e do ambiente

a) Prevenir acesso não autorizado, dano e interferência nas instalações físicas. Isso inclui: definir um perímetro de segurança, controles de entrada física, etc. Esses controles muitas vezes não dependem de recursos computacionais e também não são de responsabilidade apenas do pessoal de TI.

1 Fonte Wikipédia: engenharia social em segurança da informação ser refere à pratica de interações humanas para que pessoas revelem dados sensíveis sobre um sistema de computadores ou de informações.

b) Deve-se ter formalizada política quanto à circulação de papéis, inclusive aqueles deixados na impressora por tempo suficiente para serem acessados por outros empregados, eventualmente não autorizados, e principalmente, no manuseio dessa informação impressa.

c) Gerenciamento de mídias removíveis que devem ser controladas fisicamente e armazenadas em local seguro.

d) Descarte de mídia. Deve haver procedimentos para o descarte seguro de mídias (papel, fitas, disquetes, CD, etc.).

e) Contratos: toda troca de informação institucional entre empresas deve ser mediada por um contrato que especifique as responsabilidades quanto à segurança da informação de ambas as partes.

A Segurança da Informação[2] é uma corrente e a pessoa é o elo mais frágil. O sucesso depende do fortalecimento deste elo, na cultura da Segurança da Informação. Isto pode ser obtido mediante um programa contínuo de formação de pessoas e fomento desta cultura, de forma a proteger as informações e, para que esta proteção seja eficaz, os conceitos de segurança e as políticas desenvolvidas devem ser compreendidos e seguidos por todos, independentemente de seu nível hierárquico ou sua função na entidade.

2 Texto Gestão da Segurança a Informação da Comissão Tecnica Nacional de Governança da Abrapp publicado na Revista do 31º Congresso Brasileiro dos Fundos de Pensão, novembro de 2010.

7. GESTÃO DE RISCOS

É certo que as entidades estão cada dia mais interconectadas e compartilham um volume enorme de informações com clientes, fornecedores, consultorias, empregados e, neste ambiente, a Gestão de Riscos é fundamental para garantir o bom funcionamento da EFPC e engloba a Segurança da Informação, já que hoje a quantidade de vulnerabilidades e riscos, que podem comprometer as informações da entidade, é cada vez maior.

Ao englobar a Gestão da Segurança da Informação, a Gestão de Riscos tem como principais desafios proteger um dos principais ativos da EFPC – a informação – assim como a reputação e a marca da entidade; implementar e gerir controles que tenham como foco principal os objetivos do negócio; promover ações corretivas e preventivas de forma eficiente; garantir o cumprimento de regulamentações e gerir os processos de gestão da Segurança da Informação.

Entre as vantagens de investir na Gestão de Riscos voltada para a Segurança da Informação estão a priorização das ações de acordo com a necessidade e os objetivos da empresa e a utilização de métricas e indicadores de resultados.

A implementação das práticas de segurança da informação deve estar fundamentada e baseada na melhor relação entre os riscos inerentes aos processos, os controles que mitigarão tal exposição e os custos vinculados a estas iniciativas.

8. METODOLOGIAS

É importante salientar que não existe a definição de uma metodologia ou abordagem ideal, essa determinação vai depender do porte e complexidade das atividades das EFPC.

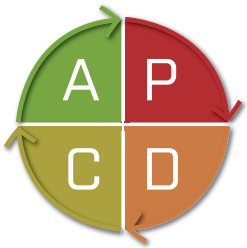
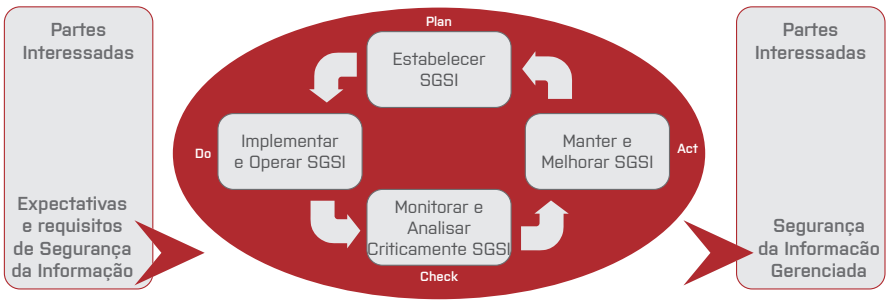


Figura 2

8.1. PDCA

O modelo PDCA (*Plan, Do, Check, Act* – Planejar, Executar, Checar e Agir) é a metodologia proposta pela ISO 27001 (padrão e referência internacional para a gestão da Segurança da Informação), para melhoria contínua de um Sistema de Gestão da Segurança da Informação - SGSI e consiste em quatro etapas.

Na abordagem para o processo do SGSI são definidas as principais ações



para cada uma das etapas do PDCA.

Figura 3 - Fonte: Modelo PDCA aplicado aos processos do SGSI – NBR ISO 27001

P	*PLAN* (planejar) Estabelecer o SGSI	Estabelecer política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
D	*DO* (fazer) Implementar e operar o SGSI	Implementar e operar política, controles, processos e procedimentos do SGSI.
C	*CHECK* (checar) Monitorar e analisar criticamente o SGSI	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para análise crítica pela direção.
A	*ACT* (agir) Manter e melhorar o SGSI	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Quadro 1 - Fonte: Atividades do PDCA – NBR ISO 27001

As fases do PDCA são sequenciais, mas não necessariamente possuem um fim, isto quer dizer que, conforme estruturamos o SGSI e conhecemos melhor a empresa podem surgir novas necessidades de mudanças no planejamento e na operação do SGSI.

Os controles, manuais e políticas do SGSI, devem ser sempre reavaliados e modificados de acordo com as mudanças do ambiente ou alterações nos processos de trabalho, por isso o uso do ciclo PDCA.

Para implementar e operacionalizar o SGSI, deve-se:

- Definir um plano de tratamento de riscos que identifique as atividades de gestão, recursos, responsabilidades e prioridades para gerir os riscos da segurança de informação;
- Definir e medir a eficácia e eficiência dos controles;
- Implementar programas de formação e sensibilização;
- Implementar procedimentos e outros controles capazes de detectarem e responderem a potenciais incidentes na segurança da informação.

8.2. SEIS SIGMA

Seis Sigma ou Six Sigma (em inglês) é um conjunto de práticas originalmente desenvolvidas pela Motorola para melhorar, sistematicamente, os processos ao eliminar defeitos. Seis Sigma também é definido como uma estratégia gerencial para promover mudanças nas organizações, fazendo com que se chegue a melhorias nos processos, produtos e serviços para a satisfação dos clientes. Diferente de outras formas de gerenciamento de processos produtivos ou administrativos o Seis Sigma tem como prioridade a obtenção de resultados de forma planejada e clara, tanto de qualidade como principalmente financeiros. (Fonte: Wikipédia)

O objetivo principal do Seis Sigma (que é um termo estatístico que mede o quanto o processo se distancia da perfeição) é a melhoria do desempenho do negócio através da melhoria do desempenho de processos. O Seis Sigma leva em conta fundamentos que estão ligados a questões gerenciais, considera o negócio, seu tamanho, suas características específicas e a cultura da organização, visando a melhoria que agregue valor ao cliente, podendo ser aplicado a problemas localizados.

A metodologia recomenda a formação de um time de trabalho e cada organização pode definir o grupo que melhor se adeque à sua realidade. Nesse caso (SGSI), é preciso que se crie um grupo multidisciplinar, envolvendo membros de várias áreas.

A abordagem do Seis Sigma, promove a qualidade através do princípio de promoção de melhoria contínua, embora esta seja uma abordagem amplamente estratégica. O método mais utilizado para a implantação dos Seis Sigma é o DMAIC (Definir, Medir, Analisar, Implementar e Controlar).

8.3. DMAIC

É uma metodologia utilizada para projetos focados em melhorar processos de negócios já existentes.

O DMAIC é dividido em cinco etapas: *Define* (Definir), *Measure* (Medir), *Analyze* (Analisar), *Improve* (Melhorar) e *Control* (Controlar).

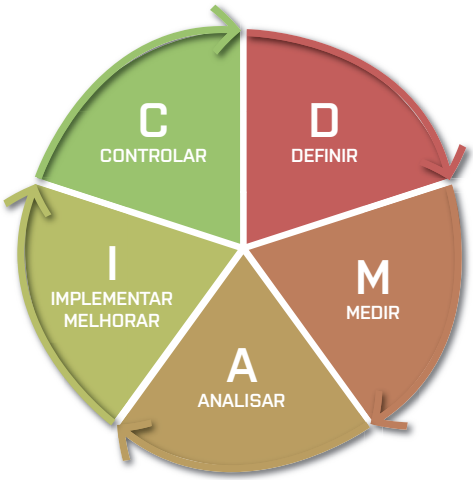


Figura 4

DEFINE (Definir) – É a primeira fase do ciclo e abrange ações relacionadas à mensuração do desempenho de processos, nessa fase devem ser respondidas algumas perguntas como: Qual é o problema a ser abordado? Qual a meta a ser atingida?

MEASUE (Medir) – Essa é a fase na qual o problema deve ser delimitado, focando-o. Para isso, podem ser utilizadas as ferramentas estatísticas que medem o desempenho dos processos. Um exemplo dessas ferramentas é a Estratificação, que Werkema (2004) define como a observação do problema sob diferentes aspectos, isto é, no grupamento dos dados sob vários pontos de vista, de modo a focalizar o problema, em relação ao tempo, ao local, ao tipo, entre outros. Outra ferramenta que pode ser utilizada é o Diagrama de Pareto, para que se possa analisar o impacto das várias partes do problema, podendo assim identificar o problema prioritário.

ANALYSE (Analisar) – É a fase na qual se deve determinar as causas fundamentais do problema. Para isso são aplicadas ferramentas como o *Brainstorming*, que segundo Aguiar (2002) é uma técnica utilizada para a geração de ideias provenientes de um grupo de pessoas, e os fluxogramas, que consiste em esquema que facilita a visualização de todas as etapas e características do processo.

IMPROVE (Melhorar) – é a quarta fase do método, e com ela se pretende identificar as soluções potencias para os problemas, para tal são utilizadas

algumas ferramentas já empregadas em outras fases como o *Brainstorming*, agora visando não mais a identificação do problema, mas sim da solução. Após a identificação das possíveis soluções devem-se priorizar as soluções potenciais, e para diminuir o risco, essa possível solução deve ser testada em pequenas escalas, sendo uma ferramenta eficiente, a simulação.

CONTROL (Controlar) – Se os testes em pequena escala foram satisfatórios, deve-se então implantar a melhoria, e após isso, verificar se a melhoria está trazendo os efeitos esperados para o processo. Para tanto, utilizam-se diversos mecanismos para monitorar continuamente o desempenho do processo.

A metodologia DMAIC está focada na robustez e simplificação dos processos, de forma a assegurar a redução do nível de defeitos, o aumento da satisfação dos clientes e da lucratividade da organização

No que se refere ao SGSI, para cada etapa[3] do DMAIC são recomendadas ações:

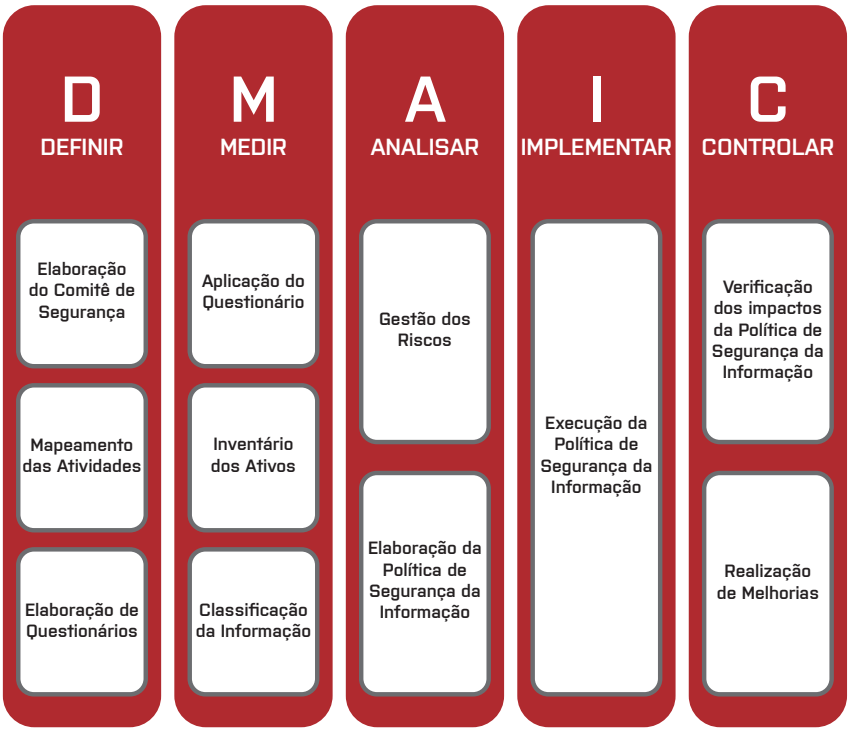


Figura 5

3 Artigo do XXVIII Encontro Nacional de Engenharia de Produção, realizado pela ABEPRO, 2008.

8.3.1. Comitê de Segurança

Este comitê deve ser formado por pessoas que irão supervisionar o processo de implantação e tomar todas as decisões que vão desde a viabilidade até avaliação do projeto. É muito importante que faça parte desse comitê, pessoas da Direção Geral trabalhando de forma atuante dentro da organização e que exerçam o poder de decisão.

8.3.2. Mapeamento das Atividades

Esta etapa pode ser realizada através de entrevistas, técnicas de *Brainstorming*, procurando identificar o problema alvo que será resolvido. Esse diagnóstico inicial será essencial para o mapeamento da segurança da informação. Para auxiliar, nessa fase, pode ser utilizado o diagrama de espinha de peixe (ou diagrama de Ishikawa) uma das ferramentas usadas pelo Seis Sigma que permite compreender as causas raízes para o problema alvo a ser resolvido. Pode ser utilizado nesta fase, também, a técnica da "situação hipotética", que é uma maneira original de redefinir o problema através de um situação hipotética na qual se faz perguntas como "o que aconteceria no setor se um determinado ativo estivesse indisponível?", essa técnica é útil para definir quais ativos são vitais para o fluxo normal de funcionamento na organização.

8.3.3. Elaboração de Questionários

A partir dos mapeamentos das atividades e de problemas alvos identificados sugere-se a elaboração de questionários com objetivo de identificar o grau de satisfação do usuário na realização dessas atividades mapeadas e identificar a percepção que a organização ou setor possui nas questões relacionadas à segurança da informação.

A utilização de instrumentos como questionários, entrevistas, entre outros, para a captação de percepções dos usuários de sistemas de informação quanto à sua segurança tem o intuito de minimizar a animosidade, normalmente, causada pela implementação das políticas de segurança da informação e também, considerar questões pertinentes à compreensão das relações sociais no âmbito organizacional, propondo uma análise comportamental dos usuários frente à segurança da informação (MARCIANO & MARQUES, 2006). O resultado deste questionário servirá como base a elaboração da política de segurança e o nível de trabalho que será feito em relação ao programa de adesão e/ou conscientização a esta política.

8.3.4. Aplicação do Questionário

Nesta etapa, será necessária a aplicação dos questionários com base

no mapeamento das atividades, obtendo assim o grau de satisfação e percepção sobre aspectos relacionados com à segurança da informação.

8.3.5. Inventário dos Ativos

Nesta etapa, recomenda-se a realização do inventário dos ativos que consiste em identificar quais são os ativos (tecnologias, processos, informação) importantes para o fluxo de funcionamento da organização, onde podem ser identificados níveis de ameaças, vulnerabilidades e probabilidade de riscos sobre determinado ativo.

8.3.6. Classificação da Informação

Neste estágio, quando forem avaliados os ativos da informação importantes para a organização, sejam eles físicos ou digitais, convêm estabelecer sua classificação quanto ao critério de tratamento, que segundo FERREIRA & ARAÚJO (2006), pode ser definida como informação pública (comum a todos), informação interna (somente dentro da organização ou setor) e informação confidencial (somente por pessoas autorizadas).

Como resultado desta fase deveremos também identificar o nível de segurança atual, para posteriormente, estabelecer sua melhora.

8.3.7. Gestão dos Riscos

Nesta fase, sugere-se a realização da análise dos riscos que serão priorizados. Conjuntamente, recomenda-se uma das ferramentas do programa Seis Sigma: o FMEA (*Failure Mode and Effect Analyses*) que é utilizado usualmente para descobrir, visualizar e priorizar as causas do problema a ser tratado (AGUIAR, 2006).

Segundo Campos (2007), uma das formas de priorizar o tratamento dos riscos é através do principio de Pareto, o qual determina que cerca de 20% das causas geram 80% das consequências. Desta maneira, não é necessário tratar todos os riscos, mas aqueles que representam uma importância mais significativa para o organização ou para o setor que está sendo tratado.

8.3.8. Elaboração da Política de Segurança da Informação

A elaboração da política dependerá das fases anteriores e principalmente diante das conclusões da gestão de riscos onde terão sido apontados os riscos mais prioritários e urgentes que precisam ser abordados na política, cabendo ao comitê de segurança assinalar quais pontos serão formalizados neste documento, como também a sua aceitação.

A Política de Segurança da Informação (PSI) é composta por um con-

junto de diretrizes que norteiam a gestão de segurança da informação, podendo ser subdividida em normas ou procedimentos, dependendo da complexidade e do nível de detalhamento requerido. O comitê de segurança revisará os documentos e efetuará sua aprovação permitindo sua execução e divulgação.

8.3.9. Execução da Política de Segurança da Informação

Nesta fase, se dará a execução e divulgação da política de segurança de informação que fora aprovada pelo comitê de segurança[4]. É muito importante que esta fase conte com a aplicação de um programa de conscientização e que os usuários da organização ou setor em que estiver sendo aplicada a política sejam treinados e conscientizados de forma que a segurança da informação faça parte da cultura organizacional. Algumas formas para estabelecer a prática de divulgação da política é o uso de e-mails, painéis, páginas intranet, reuniões, entre outras. (NAKAMURA & GEUS, 2007).

8.3.10. Verificação dos impactos da Política de Segurança da Informação

Esta etapa visa verificar os impactos e a adesão dos usuários da política de segurança da informação, mediante questionários realizados na etapa inicial, observando se houve aprendizagem e entendimento quanto aos questionamentos realizado, inicialmente. Essa etapa é importante, pois a análise comparativa entre as fases incial e atual, será decisiva para formulação de possíveis ações corretivas.

8.3.11. Realização de Melhorias

Chegando ao fim das etapas do DMAIC o objetivo é realizar o giro no processo para que se tenha sempre a continuação de todas as atividades de implantação de segurança da informação, seguindo desta maneira, o princípio do modelo de estabelecer e manter um ciclo contínuo e evolutivo de melhoria.

Com isso ao final da etapa "controlar" é verificado se houve ou não melhoria e se foi identificada alguma evolução e aprendizagem por parte dos usuários. E, a partir desta constatação é reiniciado o ciclo realizando, assim, as demais fases subsequentes, procurando identificar os problemas encontrados e prover os devidos ajustes.

4 Não existindo um Comitê de Segurança como órgão formal na estrutura da entidade, deve-se observar a competência estatutária.

9. PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

Programa de Segurança de Informação é um conjunto coordenado de atividades, projetos e iniciativas para implementar a estratégia de Segurança da Informação.

A implementação da prática de Segurança da Informação no âmbito da organização compreende uma sequência de ações importantes e indispensáveis.

Inicialmente, é necessário identificar e examinar as atividades de negócio da organização e a influência que as informações e respectivos meios e ambientes em que são tratadas exercem junto a essas atividades, visando o dimensionamento do nível de Segurança da Informação necessário.

Em seguida, deve-se avaliar o nível de Segurança da Informação existente e praticada na organização, identificando mecanismos, sistemas e ferramentas utilizadas, realizando os necessários testes de vulnerabilidades.

O Programa de Segurança de Informação envolve treinamento, conscientização e adequação dos procedimentos internos que garantam a segurança e, também, a contingência em caso de ocorrência de evento que a coloque em risco.

Através dessa estrutura, das obrigações e indicadores propostos em um Programa de Segurança da Informação, a entidade desenvolverá uma capacidade maior de atender a requisitos legais, estando em conformidade com normas e leis pertinentes.

Abaixo, um modelo de Programa, com o conteúdo e respectivas atividades, projetos ou iniciativas:

a) Assegurar informações confidenciais em seu quadro de colaboradores.

- Reforçar a importância de assegurar informações confidenciais em seu quadro de colaboradores.
- Treinamento periódico, e reciclagem por meio de campanhas, eventos, palestras e workshops.
- Criação de um Manual de Conduta que reúna todas as políticas que o colaborador deva saber sobre sua postura dentro da organização.

b) Medir o grau de eficácia da política de segurança.

- Realizar vistorias no ambiente físico, testes de vulnerabilidade, além de simulações de ataques digitais para medir o nível de segurança dos sistemas da Entidade e da cultura de seus colaboradores.

c) Desenvolver o Programa com a cooperação e suporte da alta gestão organizacional.

- Política de Segurança da Informação aprovado pelo Conselho Deliberativo estabelecendo a implementação de um Programa contínuo.

d) Para o sucesso da implementação do Programa de Segurança da Informação é importante que sejam adequadamente identificados e definidos as obrigações e papéis funcionais e os seus respectivos indicadores de desempenho.

As principais obrigações e Papéis são:

- Avaliação de Ameaças e Vulnerabilidades;
- Gerenciamento de Incidentes e Vulnerabilidades;
- Requisitos Legais e Regulamentações;
- Estratégia;
- Políticas, princípios, procedimentos e normas de Segurança da Informação;
- Continuidade de Negócios e Recuperação de Desastres;
- Educação e Comunicação;
- Governança do Programa;
- Arquitetura e Modelagem da Segurança da Informação;
- Avaliação e Capacidade Tecnológica;
- Efetividade e Análise dos Indicadores de Desempenho;
- Comitê de Segurança da Informação; e
- Interações Organizacionais.

e) Para tornar mais robustos os processos que envolvem a classificação de informação, segregação de perfil e gerenciamento de identidade.

- Revisão de atividades.

f) Alinhamento estratégico das iniciativas de Segurança com os objetivos de negócio (da organização) se torna vital na elaboração do Programa.

- Através das ações de governança (corporativa, de tecnologia da informação, de segurança da informação, etc.). Estas ações favorecem o entrosamento das operações (negócios, financeiras, logística, tecnologia da informação, segurança da informação, etc.) entre si.

10. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é o documento principal que define as diretrizes e a filosofia a ser seguida com relação ao uso e à proteção da informação.

Principais diretrizes a serem observadas:

a) Na gestão da informação, a disponibilidade, a integridade, autenticidade e a confidencialidade são garantidas nos processos de coleta, armazenamento, processamento, distribuição e descarte;

b) Na gestão, custódia e uso das informações é preservada sua confidencialidade, considerando proibido tudo aquilo que não for explicitamente permitido;

c) Planos de contingência são desenvolvidos, documentados, homologados, testados periodicamente e aprovados para ativação no caso de previsão, suspeita ou ocorrência de situações que comprometam a sua integridade, a sua disponibilidade e a continuidade das atividades da EFPC;

d) A classificação da informação é obrigatória na EFPC para todo dado e informação produzida por ela ou sob sua custódia, independentemente do suporte ou da forma utilizada para o seu armazenamento ou transmissão;

e) Impactos financeiros operacionais ou de imagem, decorrentes de classificação incorreta ou não classificação, são de inteira responsabilidade do gestor da informação;

f) O nível de classificação da informação é definido em função do seu grau de sigilo e dos impactos da sua disseminação por pessoas não autorizadas;

g) A classificação da informação possui caráter temporário e é revista pelo gestor, a partir de mudança quanto ao grau de sigilo;

h) O nível de classificação da informação considera não somente o seu aspecto individual, mas as informações a ela agregadas;

i) Nos casos de subtração, violação ou divulgação indevida de informações, a ocorrência é analisada sob o aspecto legal e disciplinar, imputando responsabilização, e sob o aspecto técnico, corrigindo vulnerabilidades;

j) A responsabilização pela divulgação de informação incompatível com o grau de sigilo atribuído pelo gestor é daquele que fizer a divulgação indevida;

k) Na contratação de serviços ou de pessoas e no relacionamentos com colaboradores, contratados e estagiários devem ser requeridos os mesmos quesitos de segurança adotados pela EFPC;

l) Questões sobre segurança da informação são disseminadas por meio de programas permanentes de conscientização de abrangência geral ou cursos de capacitação técnica para os usuários diretamente envolvidos na utilização dos recursos;

m) Definir regras de manutenção e guarda dos documentos no ambiente de trabalho (conhecido como "mesa limpa");

n) Definir as responsabilidades nos diversos níveis da organização quanto à segurança da informação; e

o) Definir claramente as consequências para infringências à política de segurança da informação.

11. CLASSIFICAÇÃO DA INFORMAÇÃO

É o processo de identificar e definir critérios adequados de proteção das informações, considerando o seu grau de sigilo. Assim, todo o documento gerado ou recebido na EFPC deve ser classificado.

A seguir, um modelo de classificação que pode variar entre as entidades:

TIPO	CLASSIFICAÇÃO	DESCRIÇÃO
Pública	00	Informações que podem ser de conhecimento público.
Corporativa	10	Informações cujo conhecimento é do interesse de toda a EFPC e podem ser divulgadas sem restrição, apenas para o público interno.
Interna	20	Informações de conhecimento exclusivo do corpo de funcionários da EFPC, podendo ser divulgadas para o público externo com autorização do gestor ou exigência legal.
Restrita	30	Informações que requerem cuidados especiais quanto à preservação de seus atributos e cuja divulgação indevida sujeita a EFPC a riscos consideráveis dirigidas ao gestor da unidade.
Confidencial	40	Informações cuja preservação de seus atributos seja fundamental para a continuidade dos negócios e cuja divulgação sujeita a Entidade a riscos muito elevados. Tratam-se de informações sigilosas, pessoais e estratégicas da EFPC.

Quadro 2

12. LEVANTAMENTO DA INFORMAÇÃO

A partir dos principais processos inerentes às atividades desenvolvidas pelas EFPC, as informações geradas deverão ser levantadas, relacionadas e classificadas conforme seu grau de sigilo (níveis definidos no item 11).

Como sugestão de níveis de classificação, relacionamos nos quadros em sequência (3A - 3M), as informações mais comuns, oriundas dos processos de uma EFPC, identificando seu grau de sigilo e destinatário da informação, considerando as etapas normais de fluxo.

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
ARRECADAÇÃO Gerir as informações cadastrais dos participantes, o recebimento e o processamento das contribuições e a conciliação da arrecadação	Fichas cadastrais dos participantes	Arquivo	40
	Mapa resumo	Arrecadação	30
	Ficha financeira	Participante, Área de Atuária e Benefício	40
	Informações financeiras para participantes (internet e impresso)	Participante	40
	Demonstrativo de contribuição anual (autopatrocinado)	Autopatrocinado	40
	Dados financeiros dos participantes para a internet	Participante	40
	Recebimento e individualização das contribuições	Arrecadação	40

Quadro 3A

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
AUDITORIA Responder pelo acompanhamento das atividades de fiscalização e controle dos órgãos externos e de empresa de auditoria independente; realizar auditoria interna; acompanhar o processo de auditoria externa e a implementação das recomendações	Relatórios de auditoria interna	Conselhos e Diretoria Executiva	40
	Relatórios de auditoria externa	Conselhos e Diretoria Executiva	30
	Plano anual de atividades de auditoria interna	Conselhos e Diretoria Executiva	40
	Cronograma de trabalho da auditoria independente	Conselhos e Diretoria Executiva	40
	Plano anual de atividades de auditoria externa	Conselhos e Diretoria Executiva	40

Quadro 3B

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
BENEFÍCIOS Gerir a concessão, manutenção, resgate e portabilidade de benefícios	Folha pagamento benefícios	Tesouraria	40
	Insumo para DIRF de assistidos	Assistidos	40
	Informe de rendimentos para assistidos	Assistidos	40
	Informe de rendimentos para participantes que resgataram reserva	Ex-participante	40
	Solicitações de concessão de benefícios	Arquivo	30
	Pedidos de auxílio doença	Arquivo	30
	Processos de saída de recursos por portabilidade	Arquivo	40
	Processos de solicitação de resgate	Arquivo	40
	Extratos previdenciários	Participante	40

Quadro 3C

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
CONTROLADORIA E TESOURARIA Gerir as informações gerenciais, o fluxo de caixa, os recolhimentos tributários e demais pagamentos e recebimentos.	Demonstrativo de população	PREVIC,Abrapp, Conselho Fiscal	20
	Disponibilidade e necessidade de caixa	Diretoria Executiva	40
	Relatório de previsão orçamentária e do orçamento geral	Diretoria Executiva	30
	Relatório de execução orçamentária	Diretoria Executiva	30
	Caderno de informações gerenciais	Conselhos e Diretoria Executiva	30
	Divergência entre os valores orçados e os realizados	Diretoria Executiva	30
	Autorizações para os pagamentos	Arquivo	30
	Fluxo de caixa	Diretoria Executiva	40
	Saldo bancário e disponibilidade	Diretoria Executiva	40
	Conciliações bancárias	Arquivo	40
	Fechamento do caixa	Arquivo	40
	Movimento financeiro consolidado	Área de Contabilidade	20
	Informações mensais para os conselhos	conselhos	30
	Relatório gerencial mensal	Patrocinadoras	20

Quadro 3D

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
CONTABILIDADE Gerir o processo contábil da entidade, registrar e controlar atos e fatos contábeis, calcular cotas, elaborar demonstrativos e declarações fiscais.	Balancetes mensais	PREVIC, Diretoria Executiva, Patrocinador, Auditoria Externa	10
	Demonstrações contábeis financeiras (anual)	Diretoria Executiva, Conselhos e PREVIC	20
	Relatório de conciliação das contas patrimoniais e de resultado	Auditoria Externa, Área de Tesouraria	20
	Valor da cota para os planos de benefícios	Áreas Benefício e Atuária	20
	Declarações oficiais exigidas pela receita federal do brasil	Receita Federal do Brasil	20
	Cálculo dos recolhimentos dos tributos e da TAFIC	Área de Tesouraria	20

Quadro 3E

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
INVESTIMENTOS Gerir os investimentos dos recursos dos planos de benefícios administrados pela entidade	Política de investimento	PREVIC, Conselhos e participantes.	20
	Estudos de ALM	Conselhos, Diretoria Executiva, Área de Atuária	20
	Demonstrativos de investimentos	PREVIC, Auditoria Externa	20
	Parâmetros de exposição ao risco	Conselhos, Diretoria Executiva e Auditoria Externa	20
	Relatórios sobre as alternativas de investimento	Comitê Financeiro	40
	Documentos de autorização para investimento	Órgão Investidor, Comitê Financeiro	40
	Rentabilidade dos investimentos	Conselhos, Diretoria Executiva, Participantes, Patrocinadora e Abrapp	20
	Relatório de acompanhamento do cumprimento da política de investimento	Conselhos, Diretoria Executiva e Comitê Financeiro.	20
	Demonstrativo da divergência não planejada	PREVIC, Conselhos, Diretoria Executiva e Comitê Financeiro.	20

Quadro 3F

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
ATUÁRIA Modelar planos de benefícios e administrar os aspectos atuariais	Avaliação atuarial	PREVIC, Diretoria Executiva, Patrocinadoras	20
	Testes de aderência das premissas e hipóteses atuariais	PREVIC, CD, Diretoria Executiva, Patrocinadoras	20
	Simulação atuarial de benefícios	Participante	30
	Nota técnica atuarial	PREVIC	20
	Reservas matemáticas	Área de Contabilidade	20
	Cálculos de revisão de percentuais	Patrocinadora, Participantes	30
	Revisão do plano de custeio	PREVIC, Patrocinadora, Área de Arrecadação	20
	Estudos atuariais	Diretoria Executiva, Clientes Efetivos e potenciais	20
	Cálculo da jóia atuarial	Participante	30
	Regulamentos dos planos	PREVIC, EFPC, Patrocinadora e Participantes	00
	Cálculo de benefício	Área de Benefício	30

Quadro 3G

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
RECURSOS HUMANOS E ADMINISTRATIVO Gerir o processo de administração e desenvolvimento dos recursos humanos e o patrimônio da entidade	Folha pagamento empregados	Tesouraria	40
	Folha de ajustes do ponto	Arquivo	20
	Contratos com fornecedores diversos	Arquivo	20
	Manual de organização e regimentos internos	Corpo Funcional	10
	Manual de alçada	Corpo Funcional	10
	Documentos institucionais	Corpo Funcional	10
	Avaliação dos fornecedores de bens e serviços	Gerências	30
	Cadastro e dossiê dos funcionários	Arquivo	30
	Processos de admissão e desligamento	Diretoria Executiva	30
	Plano de cargos e salários	Diretoria Executiva, Funcionários	20
	Prestação de contas dos empregados	arquivo	30
	Pesquisa de satisfação de patrocinadoras e participantes	Diretoria Executiva, Funcionários	10
	Informações cadastrais dos fornecedores	Gerências	20
	Documentos de destacamentos, diárias, bilhetes aéreos, prestação de contas	Arquivo	30
	Documentos relativos aos treinamentos	Arquivo	$30
	Documentos relativos aos planos de saúde, odontológicos de medicamentos	Arquivo	$30
	Inventários	Diretoria Executiva	30

Quadro 3H

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
RELACIONAMENTO Gerir o relacionamento e os negócios com os participantes e garantir sua manutenção e fidelização	Documentos campanhas de adesão	Patrocinadoras e Participantes	30
	Contrato de adesão	Patrocinadoras	30
	Manual do participante	Participantes	20
	Scripts	Participante e Central de Atendimento	20
	Propostas de novos planos para participantes potenciais	Clientes Potenciais	40
	Cartilha de perguntas e respostas	Participantes	20
	Planos de ação elaborados	Diretoria Executiva e Conselhos	30
	Relatório de riscos	Diretoria Executiva	30

Quadro 3I

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
JURÍDICO Gerir atividades de natureza jurídica, assessorar e representar juridicamente a entidade, em juízo e extrajudicialmente	Ações judiciais	Diretoria Executiva	40
	Ações administrativas	Diretoria Executiva	40
	Relatório dos processos contenciosos	Diretoria Executiva e Conselhos	30
	Relatório dos processos administrativos	Diretoria Executiva	40
	Pareceres técnicos	Diretoria Executiva	30
	Contratos de confissão de dívida	Diretoria Executiva	40
	Minuta de documentos institucionais	Diretoria Executiva	30
	Relatório de prestação de contas de jurídicos terceirizados	Diretoria Executiva	40
	Relatório de controle de jurídicos terceirizados	Diretoria Executiva	40
	Relatórios jurídicos com ações classificadas e atualizadas para constituição de provisão	Diretoria Executiva	40
	Contratos dos escritórios de advocacia terceirizados	Diretoria Executiva	40

Quadro 3J

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
MARKETING E COMUNICAÇÃO Gerir o processo de definição e implementação das estratégias de marketing interno e externo	Relatório anual de informações aos participantes e assistidos	Participantes	00
	Plano anual de comunicação	Diretoria Executiva	10
	Planos de comunicação para campanhas	Diretoria Executiva	30
	Informativo em pauta	Corpo Funcional	10
	Relatório anual de atividades da diretoria	Conselhos e Diretoria Executiva	10
	Boletim eletrônico mensal	Participantes e Assistidos	00

Quadro 3K

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
SECRETARIA EXECUTIVA Gerir a agenda executiva da entidade, organizar e secretariar as reuniões das diretorias, conselhos e comitês	Cadastros dos conselheiros	Arquivo	40
	Cadastros dos diretores	Arquivo	40
	Atas das reuniões e registros de deliberações dos conselhos	Arquivo	40
	Atas das reuniões e registros de deliberações da diretoria executiva	Arquivo	40
	Cadastro de auditores, atuários, contadores e advogados	Arquivo	40
	Documentos de nomeações	Arquivo	40
	Atas das reuniões dos comitês	Arquivo	40

Quadro 3L

PROCESSO	INFORMAÇÃO	DESTINO	CLASSIFICAÇÃO
SETOR ADMINISTRATIVO Gerir o fluxo de correspondências e trânsito de documentos e pessoas e o património físico da entidade	Inventário dos bens patrimoniais da efpc	Arquivo	20
	Solicitações de materiais e equipamentos	Arquivo	20
	Sistema de protocolo	Arquivo	20

Quadro 3M

13. TRATAMENTO DA INFORMAÇÃO

Abrange todo o ciclo de vida da informação: criação, manuseio, armazenamento, distribuição, transporte e descarte, garantindo sua confidencialidade, integridade e disponibilidade.

Como sugestão, relacionamos nos quadros 4 (4A - 4H) os critérios de classificação e tratamento da informação em função da classificação.

CLASSIFICAÇAO					
OBJETIVO					
Estabelecer normas para processamento, classificação, reclassificação, transmissão, armazenagem e destruição das informações de acordo com o grau de sigilo, independentemente do suporte ou forma em que é armazenada, veiculada ou transportada.					
PRODUÇÃO DA INFORMAÇÃO					
Preferencialmente, nas instalações da EFPC, não sendo permitido em lugares públicos.					
CLASSIFICAÇÃO DA INFORMAÇÃO – GRAU DE SIGILO					
	00 PÚBLICA	**10 CORPORATIVA**	**20 INTERNA**	**30 RESTRITA**	**40 CONFIDENCIAL**
	Podem ser de conhecimento público	Conhecimento é do interesse de toda a EFPC	Conhecimento exclusivo do corpo de funcionários da EFPC	Requerem citação explícita das pessoas ou grupos autorizados	Informações pessoais e estratégicas, com citação explícita das pessoas ou grupos autorizados

Quadro 4A

DISPONIBILIDADE					
	00 PÚBLICA	**10 CORPORATIVA**	**20 INTERNA**	**30 RESTRITA**	**40 CONFIDENCIAL**
Todas as informações	Disponível para o público interno e externo	Apenas para o público interno	Apenas para o público interno, podendo ser disponibilizada para fora da entidade apenas com base em interesse negocial (aprovado pelo gestor da informação) ou requisição legal	Disponível para os funcionários da Entidade. Quando houver necessidade, terceiros poderão ter acesso controlado e monitorado. Não deve ser encaminhada para fora da Entidade	Disponível para funcionários da Entidade, sendo obrigatório indicar o nome das pessoas ou cargos que poderão acessar a informação. Não deve ser encaminhada para fora da Entidade

Quadro 4B

TRANSMISSÃO/DIVULGAÇÃO					
	00 PÚBLICA	**10 CORPORATIVA**	**20 INTERNA**	**30 RESTRITA**	**40 CONFIDENCIAL**
Correio	Sem preocupações adicionais	Usar correspondência envelopada registrada	Usar correspondência envelopada registrada e que possa ser rastreada	Uso desaconselhado. Caso necessário, deve haver anuência prévia do gestor da informação e enviada correspondência que possa ser rastreada, de preferência com portador e recibo de entrega, ou, na falta, SEDEX ou correlato	Não é permitido, a não ser em casos extremos, com a anuência do gestor da informação, observados os cuidados das restritas
Correio eletrônico E-mail corporativo (destinatário interno)	Sem precauções adicionais			Utilizar com precaução	Uso desaconselhado
Correio eletrônico E-mail corporativo (destinatário externo)	Sem precauções adicionais	Usar, apenas, quando houver interesse negocial, aprovado pelo gestor da informação		Utilizar precaução	Não é permitido
Fax	Verificar a discagem correta do número			Notificar o destinatário antes de passar o fax e confirmar, posteriormente, a recepção correta do mesmo	Vedado o uso
E-mail pessoal	Vedado o uso				
Sitio da internet	Sem precauções adicionais	Não é permitido, a não ser quando expressamente autorizado pela Diretoria Executiva			
Conversas em locais públicos	Sem precauções adicionais	Vedado			
Reuniões	Sem precauções adicionais	Em ambiente interno. Tomar precauções em relação ao sigilo	Atentar para que apenas as pessoas autorizadas acessem a informação		

TRANSMISSÃO/DIVULGAÇÃO (continuação)					
	00 PÚBLICA	**10 CORPORATIVA**	**20 INTERNA**	**30 RESTRITA**	**40 CONFIDENCIAL**
Telefone fixo	Sem precauções adicionais	Tomar precaução em relação ao sigilo	Tomar precaução em relação ao sigilo. Precaver-se contra a aproximação de pessoas não autorizadas	Precaver-se contra a aproximação de pessoas não autorizadas. Uso de viva-voz, apenas, em áreas fechadas	Precaver-se contra a aproximação de pessoas não autorizadas. Vedado o uso de viva voz
Celulares	Sem precauções adicionais	Tomar precaução em relação ao sigilo		Uso desaconselhado	Não é permitido. Em casos extremos, utilizar em local restrito e tom de voz moderado.
Alto-falantes	Sem precauções adicionais	Vedado			

Quadro 4C

REPRODUÇÃO					
	00 PÚBLICA	**10 CORPORATIVA**	**20 INTERNA**	**30 RESTRITA**	**40 CONFIDENCIAL**
Todas as informações	Pode ser realizada por empregado, prestador de serviço e estagiário	Permitida, desde que mantida a integridade da informação e seja para uso exclusivo no desenvolvimento das atividades profissionais		Cópias devem ser previamente autorizadas pelo gestor da informação. Atentar para a integridade e confidencialidade da informação Em caso de cópia digital, os arquivos temporários devem ser eliminados	Vedada a reprodução de todo ou parte. Permitido somente para pessoas, cargos ou grupo de pessoas autorizadas pelo gestor da informação e em processos de *backup*

Quadro 4D

ARMAZENAMENTO/GUARDA					
	00 PÚBLICA	**10 CORPORATIVA**	**20 INTERNA**	**30 RESTRITA**	**40 CONFIDENCIAL**
Impressos, formulários e anotações	Sem precauções adicionais	Guardar em local trancado		Guardar em local restrito e trancado (preferencialmente em armário de segurança) quando não estiver sendo usada. Acesso, apenas, para as pessoas que necessitam pela natureza de seu trabalho	Guardar em local restrito e trancado (preferencialmente em armário de segurança), com controle e registro de acesso. Disponível apenas para pessoal previamente autorizado pelo gestor da informação
Informações eletrônicas (em geral)	Sem precauções adicionais	Armazenamento apenas na rede corporativa	Armazenamento apenas na rede corporativa. Acesso restrito ao público interno	Armazenamento apenas na rede corporativa em ambiente compatível com a criticidade	Armazenamento apenas na rede corporativa, em locais específicos, e que possuam rotina de *backup* e registros de *log*
E-mail corporativo	Armazenamento apenas em bases corporativas				Armazenamento em bases corporativas com criptografia
Mídias removíveis	Sem precauções adicionais	Guardar em local de acesso exclusivo para público interno		Guardar em local restrito e trancado. Acesso apenas para as pessoas que necessitam pela natureza do seu trabalho	Guardar em local restrito, trancado e com controle e registro de acesso. Disponível apenas para pessoal previamente autorizado pelo gestor da informação

Quadro 4E

DESCARTE/DESTRUIÇÃO					
	00 PÚBLICA	10 CORPORATIVA	20 INTERNA	30 RESTRITA	40 CONFIDENCIAL
Impressos, formulários e anotações	Sem preocupações adicionais	Utilizar fragmentadora			
Formulários, impressos e anotações (timbrado)	Utilizar fragmentadora				
Disquetes, CD's e DVD's	Sem preocupações adicionais	Utilizar fragmentadora, perfurador ou picotar com tesoura			
Pen drive, HD externo e interno	Sem preocupações adicionais	Utilizar ferramenta corporativa para formatar a mídia antes de ser descartada			
Fitas VHS	Sem preocupações adicionais	Retirar a fita e picotar com tesoura			
Dispositivos móveis (notebooks, palm's e celulares)	Sem precauções adicionais	Utilizar ferramenta corporativa para formatar a mídia antes de ser descartada			

Quadro 4F

RECICLAGEM					
	00 PÚBLICA	10 CORPORATIVA	20 INTERNA	30 RESTRITA	40 CONFIDENCIAL
Impressos, formulários e anotações	Sem preocupações adicionais	Destruir utilizando fragmentadora antes de encaminhar para reciclagem			

Quadro 4G

REUTILIZAÇÃO					
	00 PÚBLICA	10 CORPORATIVA	20 INTERNA	30 RESTRITA	40 CONFIDENCIAL
Mídias removíveis	Sem preocupações adicionais	Utilizar ferramenta corporativa para formatar a mídia antes de ser reutilizada			
Dispositivos móveis (notebooks, palm's e celulares)	Sem preocupações adicionais	Utilizar ferramenta corporativa para formatar a mídia antes de ser reutilizada			
Impressos, formulários e anotações	Sem precauções adicionais	Vedado			

Quadro 4H

O nível da classificação deve ser indicado no canto superior direito de todas as páginas, inclusive capa (se houver), independente do meio em que se encontre (papel, capas de CD e DVD, mensagens eletrônicas, armazenadas em mídia removível e rede corporativa). Deve-se numerar, consecutivamente, as páginas indicando o número total de páginas. Para informações em meio eletrônico, o nível de classificação deve ser indicado no topo superior de cada tela. O Plano de Continuidade do Negócio – PCN consiste num conjunto de estratégias e procedimentos que devem ser adotados para eventualidade da entidade ou uma área deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

Essas estratégias e procedimentos deverão minimizar o impacto sofrido diante de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

14. PLANO DE CONTINUIDADE DE NEGÓCIOS

O Plano deve conter um conjunto de medidas que combinem ações preventivas e de recuperação e tem por objetivo manter a integridade e a disponibilidade dos dados da organização, bem como a dos seus serviços quando da ocorrência de situações fortuitas que comprometam o bom andamento dos negócios.

O PCN deve abranger aspectos como:

1. Condições e procedimentos para ativação do Plano (como se avaliar o impacto provocado por um incidente);

2. Procedimentos a serem seguidos imediatamente após a ocorrência de um incidente;

3. A instalação reserva, com especificação dos bens de informática nela disponíveis, como hardware, software e equipamentos de telecomunicações;

4. Procedimentos necessários para restaurar os serviços computacionais na instalação reserva;

5. A escala de prioridade dos processos operacionais, de acordo com seu grau de criticidade para o funcionamento da entidade;

6. Dependência de recursos e serviços externos ao negócio;

7. Pessoas responsáveis por executar e comandar cada uma das atividades previstas no PCN; e

8. Contratos e acordos que façam parte do PCN para restauração dos serviços.

Como garantia do funcionamento e eficácia, o PCN prevê a realização de:

1. Programa de conscientização das pessoas envolvidas, por meio de palestras e treinamento;

2. Testes periódicos, podendo ser integrais ou parciais; e

3. Processo de manutenção contínua.

O propósito de um PCN é permitir que a entidade recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios e, para auxiliar neste processo o *backup* dos sistemas e/ou das estações de trabalho tem um papel relevante.

A complexidade e o detalhamento da estratégia de backup dependem do porte e das necessidades de cada entidade. Porém, é necessário que se faça a classificação da informação, com atributos como permissões de acesso, data, tempo de retenção local de armazenamento, etc, de forma a minimizar o risco das informações.

A Comissão Técnica Regional Sudeste de Governança da Abrapp, coordenou a elaboração de um Guia de Boas Práticas de Continuidade de Negócios, publicado em outubro de 2012, com o objetivo de promover a adoção de boas práticas de gestão, de forma que, realizadas de maneira prudente, ética e diligente, tenhamos como foco o gerenciamento e a mitigação dos riscos.

15. TESTE DE VERIFICAÇÃO DA CONFORMIDADE DO PROCESSO DE SEGURANÇA DA INFORMAÇÃO

O teste de verificação da conformidade consiste na aplicação de um questionário básico de avaliação da segurança da informação, com o objetivo de ser um primeiro instrumento de avaliação, em nível gerencial, da efetividade do processo de segurança da informação da entidade. O questionário não cobre todos os controles que devem existir em um processo de segurança da informação, porém, ele considera os principais controles e possibilita que, com as respostas recebidas, sejam feitas recomendações de implementação de controles e/ou apontada a necessidade de uma avaliação mais detalhada.

Apresentamos no quadro 5, parâmetros para avaliação da conformidade e nos quadros 6, modelo de teste de verificação com alguns questionamentos colhidos do livro "Praticando a Segurança da Informação", de Edison Fontes.

SEGURANÇA DA INFORMAÇÃO

TESTE DE VERIFICAÇÃO DA CONFORMIDADE

INDICADOR	DESCRIÇÃO
1	Não se aplica
2	Não
3	Solução em planejamento inicial
4	Parcialmente implementada. Ainda não confiável
5	Possui o mínimo de atendimento aos requisitos
6	Prestes a ser melhorada
7	Satisfatório para situações normais
8	Está funcionando bem
9	Totalmente implementada
10	Solução implementada é referência no mercado

Quadro 5

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
Existe um documento principal da política de segurança da informação definindo as diretrizes e filosofia da entidade em relação ao uso e proteção da informação?										
A política de segurança e proteção da informação foi assinada pela Diretoria Executiva?										
Existem normativos que complementam e detalham como os objetivos descritos na política podem e devem ser alcançados?										
Existe um processo que garanta a atualidade dos normativos de segurança?										
É garantido que todos os usuários da informação conhecem os normativos existentes?										

Quadro 6A

GESTÃO DE ATIVOS

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
Existe uma política de classificação da informação que define os níveis de sigilo e indica para cada um deles como deve ser tratada a informação?										
Existe definido, para toda informação apresentada para o usuário (transação, tela, relatório, documentos), o nível de sigilo?										
Existe definido, para toda informação apresentada para o usuário (transação, tela, relatório, documentos), o gestor da informação?										
Existe definido para toda informação armazenada no ambiente computacional o custodiante da informação?										
O gestor da informação é o responsável pela liberação (ou não) do acesso à informação pelo usuário?										
Existe um procedimento definido para o descarte de equipamentos garantindo que as informações serão devidamente apagadas antes do ativo ser liberado?										

Quadro 6B

SEGURANÇA FÍSICA E DO AMBIENTE

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
Cada pessoa tem autorização de acesso físico apenas aos ambientes que necessita acessar para desempenhar as suas funções profissionais na organização?										
O acesso físico das áreas da organização é controlado, impedindo que pessoas não autorizadas acessem ambientes em que não estão autorizadas?										
O acesso físico de cada pessoa fica registrado, permitindo uma auditoria?										
Para os ambientes restritos o controle de acesso obriga o acesso individual e evita que alguém entre "de carona" quando uma pessoa autorizada acessa o ambiente?										
Os visitantes são identificados individualmente e têm registradas sua entrada e saída dos ambientes?										
As pessoas são avisadas de que o ambiente é monitorado e gravado?										

Quadro 6C

GERENCIAMENTO DE OPERAÇÕES E COMUNICAÇÕES

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
Existe documentação dos processos e procedimentos relativos aos recursos de informação?										
No ambiente computacional existe a separação do ambiente de produção (onde estão os sistemas que suportam o negócio) em relação aos demais ambientes?										
É proibida a execução no ambiente de produção de programas em teste ou em situação de homologação?										
A passagem de programas para o ambiente de produção é feito de maneira controlada, registrada e fazendo parte de um processo de gestão de mudança?										
Todo o processo de passagem de programa para o ambiente de produção pode ser auditado?										
Os serviços prestados por terceiros são monitorados e gerenciados de maneira que possa ser feita uma avaliação desse prestador de serviço?										

Quadro 60

CONTROLE DE ACESSO

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
A identificação é única e individual para qualquer tipo de usuário?										
Há a garantia de não existência de identificações genéricas?										
A cadeia de caracteres que formam a identificação do usuário possibilita fazer a ligação com os dados complementares e descritivos deste?										
Quando a autenticação é feita através de senha, esta é secreta e de conhecimento exclusivo do usuário?										
É declarado nas políticas que o usuário é responsável pelo acesso realizado com a sua identificação e autenticação?										
Todo acesso realizado ou tentativa de acesso no ambiente computacional é gravado e guardado durante um tempo previamente definido pela segurança da informação?										

Quadro 6E

AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
É utilizada uma metodologia de desenvolvimento de sistemas, e esta é de conhecimento de todos os desenvolvedores?										
Existe na metodologia uma etapa para a especificação dos requisitos de segurança da informação, antes do desenho lógico da solução?										
A documentação exigida pela metodologia é suficiente para que outro profissional com mesmo conhecimento técnico possa substituir um desenvolvedor de sistemas?										
Existe um efetivo controle de versão para os programas e outros elementos construídos pelos desenvolvedores, garantindo a integridade dos mesmos durante o processo de desenvolvimento?										
Existem pelo menos três ambientes computacionais: de desenvolvimento, de testes e de produção?										
Quando da aquisição de produtos são considerados vários aspectos da solução, inclusive o grau de certeza da continuidade do fornecedor no mercado de tecnologia?										
Existe um processo de garantia de qualidade desde a especificação da necessidade da área de negócio?										
Existe um processo rigoroso em relação à gestão de alterações de escopo, produtos e outros elementos da solução original?										
Existem cópias de segurança suficientes para recuperação do ambiente de desenvolvimento de sistemas?										

Quadro 6F

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
Existe um processo estruturado para o tratamento de incidentes de segurança da informação?										
A prioridade de ações a ser feita em consequência de ocorrência de incidente de segurança da informação considera o negócio da informação?										
Existe formalmente um acordo de nível de serviço (SLA) para a resolução de incidentes de segurança da informação?										
Existe um canal de comunicação onde o usuário possa registrar a ocorrência de um incidente, preservando a sua identidade, porém, podendo acompanhar a pesquisa desse incidente e conclusões definidas pela Entidade?										

Quadro 6G

GESTÃO DA CONTINUIDADE DE NEGÓCIO

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
Existe um plano de continuidade de negócio para ser seguido quando da ocorrência de um desastre que indisponibilize recursos de informação?										
É realizada periodicamente uma avaliação de risco com foco nas ameaças que podem indisponibilizar recursos de informação e podem parar ou degradar em muito o desempenho da realização do negócio?										
As áreas de negócio foram responsáveis pela definição do tempo desejável para a recuperação dos recursos de informação necessários para a realização do negócio?										
São realizados testes periódicos para a utilização do plano de continuidade de negócio?										
A solução adotada foi validada pela direção executiva da Entidade e aceita formalmente?										
Existem cópias de segurança considerando aspectos de operação, de auditoria, histórico e legal guardadas de forma segura, suficientes para uma recuperação da informação?										

Quadro 6H

CONFORMIDADE

QUESTIONAMENTOS	01	02	03	04	05	06	07	08	09	10
Existe de forma explícita o conjunto de legislação, regulamentos e requisitos éticos que a Entidade é obrigada a cumprir?										
Esse conjunto de requisitos é de conhecimento dos usuários que tratam a informação da Entidade para desenvolver sistemas, proteger a mesma e definir procedimentos de recuperação dos recursos de informação?										
A área jurídica interage fortemente com a área de segurança da informação e com a área de tecnologia da informação, com o objetivo de garantir a conformidade com a legislação e demais regulamentos?										
As cópias de segurança da informação são guardadas em um local com o mesmo nível de segurança do local original?										
Havendo transporte físico da cópia de segurança, ele é realizado em embalagens específicas para esse tipo de deslocamento?										
São feitos testes periódicos das cópias de segurança da informação em relação ao acesso e à integridade da informação?										

Quadro 61

16. TRANSPARÊNCIA *VERSUS* SEGURANÇA DA INFORMAÇÃO

Para o Instituto Brasileiro de Governança Corporativa – IBGC:

> A transparência mais do que a obrigação de informar, é o desejo de disponibilizar para as partes interessadas informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. À adequada transparência resulta um clima de confiança, tanto internamente quanto nas relações da empresa com terceiros. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que conduzem à criação de valor.
>
> Há, também, o entendimento de que a transparência é o desejo de promover informações relevantes e não confidenciais de forma clara, tempestiva e precisa, incluindo informações de caráter não financeiro, conhecido como princípio de *disclosure*.
>
> Deste modo, o fato de não disponibilizar determinadas informações não implica em falta de transparência, dado que se deve preservar aquelas que são privadas, restritas e/ou confidenciais, de forma a protegê-las de uma disponibilização indevida e de utilização inadequada. Uma prática que se deve adotar, de forma a não ferir a confiança, é estabelecer um procedimento resposta, inclusive quanto ao motivo da negativa da informação.
>
> A disponibilização das informações deve estar respaldada na identificação e controles dos riscos mediante a implementação de controles internos fortes, proporcionado a devida transparência aos usuários da informação, havendo assim, a necessidade de se definir as responsabilidades pela gestão da informação.
>
> Compete ao órgão regulador das EFPC fixar condições que assegurem transparência, acesso à informação e fornecimento de dados relativos aos planos de benefícios, inclusive quanto à gestão dos respectivos recursos.

17. COMO AS ORGANIZAÇÕES ESTÃO EM RELAÇÃO À SEGURANÇA DA INFORMAÇÃO

Segundo uma pesquisa realizada pela PriceWaterHouse o número maior de incidentes combinado a um aumento paralelo no volume de dados de negócios compartilhados digitalmente, leva à proliferação da perda de dados. Dentre as categorias de dados afetados, lideram a lista os registros de funcionários e de clientes, e na terceira posição encontram-se a perda ou dano de registros internos.

A maioria das organizações atribuem os incidentes de segurança a agentes internos (funcionários ou ex-funcionários) e muitas delas não possuem um plano de resposta para lidar com esses incidentes.

Um risco importante para a segurança da informação é a expansão do uso de dispositivos móveis, como smartphones e tablets, além da tendência dos funcionários utilizarem seus próprios dispositivos (pen drive) no ambiente da empresa e, a implantação de políticas de segurança móvel não acompanha a proliferação desses aparelhos.

A computação em nuvem vem sendo uma opção crescente nas organizações e vem se discutindo a respeito da privacidade de dados neste ambiente. O que se observa é que poucas organizações têm uma política para gestão de serviços na nuvem. Outro desafio que vem ganhando visibilidade é a prevenção contra vazamento de informações.

Embora, a maioria dos envolvidos em segurança concorde que ações devam ser tomadas para melhorar a segurança da informação, encontram obstáculos como: insuficiência de investimentos, entendimento inadequado de como futuras necessidades de negócio afetarão a segurança das informações, comprometimento da liderança, sistemas de TI e informações excessivamente complexas e mal integradas.

Fato é que as organizações, por estarem se tornando alvo de ataques cada vez mais frequentes, se obrigam a aprimorar seus controles detectivos, o que pode explicar o aumento no volume de incidentes e, para combater as ameaças, o patrocínio adequado da alta administração é essencial, de forma a não comprometer o sucesso das ações de segurança e, os investimentos, que devem ser, também, alocados em tecnologia, processos e pessoas.

As EFPC, como qualquer organização, da mesma forma, estão constantemente expostas a ameaças, e quanto maiores as suas vulnerabilidades, maiores os riscos à segurança da informação e, portanto, devem identificar, avaliar, controlar e monitorar estes riscos.

18. RISCOS NOS PROCESSOS

A gestão de risco é uma atividade que, entre outras ações, descreve os possíveis entraves nos processos gerenciais que podem dificultar ou até mesmo inviabilizar os projetos dentro de uma organização. Exemplo: ataque de vírus, afetando todo o sistema de arquivos de uma entidade.

Os riscos analisados devem ser tratados, com as ações necessárias para minimizá-los. A análise de risco deve ser sempre reavaliada, para ter eficácia e produzir melhores resultados.

Outro fator importante é o registro de todos os incidentes de segurança, *logs* de eventos para análises futuras, visando que não haja reincidência de não conformidades.

Novos colaboradores precisam conhecer e estar cientes que a entidade preza pela ética, bom uso dos recursos e segurança da informação. Por isso, o departamento de Recursos Humanos, no momento da contratação, deve assegurar que eles entenderam suas responsabilidades e seus papéis, comprometendo-se em reduzir o risco de roubo, fraude, violação da segurança da informação ou mau uso de recursos.

Em projeto de SGSI, toda a entidade deve estar comprometida. Para tanto, a conscientização e treinamento dos colaboradores é uma etapa primordial no processo.

Para o SGSI ser completo, é preciso analisar vários fatores, tais como, a segurança do local, acessos, alarmes, registro de entrada e saída de pessoal, o bom uso dos computadores, política de senha, processos de *backup*. Tudo isso será descrito em política de segurança das informações que todos precisam entender, se comprometer a respeitar e, ter ciência de que, em caso de recusa, pode ser responsabilizado segundo normativos pertinentes.

Na sequência um modelo de Mapa de Risco de segurança da informação. Importante ressaltar que os riscos não se restringem ao descrito nos quadros 7 (7A - 7F).

PROCESSO	FATOR DE RISCO	IMPACTO	CONTROLE
ARRECADAÇÃO	Informações não confiáveis por problemas em sistema ou falta de verificação ou de atualização	Multa ou sanção por não atender ao artigo 18 da Res. CGPC Nº13/2004 Pagamento indevido de benefícios com erro	Verificação da consistência de dados cadastrais Atualização cadastral periódica e circunstancial
	Informações não confiáveis por falta de verificação	Não atender ao artigo 18 da Res. CGPC Nº13/2004 Cálculo de valores de contribuições e benefícios com erro	Verificação das informações fornecidas, por terceiros (patrocinadores)
	Dispor, indevidamente, de informações privadas disponibilizadas em portal.	Entidade pode ser responsabilizada pelo acesso a informações privadas por pessoa não autorizada	Política de acesso
	Manter Informações incorretas sobre os planos no sítio eletrônico do Ministério da Previdência Social	Advertência e multas, por deixar de atender ao Artigo 2º da Res. CGPC 18/2006 e Artigo 11 da Res CGPC 23/2006	Duplo check, checando as informações da entidade no site do Ministério da Previdência Social

Quadro 7A

PROCESSO	FATOR DE RISCO	IMPACTO	CONTROLE
INVESTIMENTOS	Prejuízo às negociações por utilização, por ex-diretores, de informações a que teve acesso	Multa ou sanção por não atender o Artigo 23 da LC 108/2001 e Artigo 2º da Res CGPC Nº 4/2003	Termo de conhecimento e de responsabilidade quanto ao impedimento
	Ter de aceitar operações fora dos parâmetros pretendidos por não conseguir comprovar os parâmetros efetivamente acordados	Prejuízo financeiro e/ou assunção de riscos indesejados	Gravações telefônicas
	Divulgação de informações incorretas	Abalar a credibilidade da entidade perante seu público	Procedimento de divulgação de informações contemplando a prévia análise das informações a serem divulgadas
	Informações imprecisas para as áreas	Pode gerar, dentre outros, erro de cota e demais impactos advindos desta falha	Conciliação diária e validação de informações (duplo check) previamente à disponibilização
	Ausência de evidência de fundamentação e/ou aprovação por extravio de documentação	Não demonstrar aderência à Política de Investimento e Alçadas	Documentação devidamente controlada (numeração) e arquivada

Quadro 7B

PROCESSO	FATOR DE RISCO	IMPACTO	CONTROLE
RECURSOS HUMANOS	Sofrer sanções por deixar de prestar informações e esclarecimentos definidos no §3º, artigo 41, LC nº 109/2001	Multa, podendo ser cumulada com suspensão	Controle de demandas e respostas e definição de responsabilidades
	Implantação de dados no sítio eletrônico por pessoa não autorizada	Entidade responde por erros ou omissões e por não cumprir requisitos da Instrução SPC nº 23/2008	Controle de acesso Controle dos termos de responsabilidade Atualização mensal das informações cadastrais
	Divulgação de informações restritas ou confidenciais	Prejuízos financeiros e risco de imagem pela quebra de confiança	Política de divulgação de informações e Código de conduta
	Impressão de informações restritas ou confidenciais expostos a qualquer colaborador	Acesso e uso indevido de informações restritas ou confidenciais	Sistema de impressão controlada por senha ou em impressora reservada
	Exposição de informações permitindo acesso a pessoas não autorizadas	Acesso e uso indevido de informações restritas ou confidenciais	Controle de acesso e circulação nas dependências da entidade Cultura de "mesa limpa"

Quadro 7C

PROCESSO	FATOR DE RISCO	IMPACTO	CONTROLE
RELACIONAMENTO	Sanções por deixar de atender a requerimento formal de informação, encaminhado pelo participante, ou atendê-lo fora do prazo	Advertência ou multa Artigo 84 do Decreto nº 4.942/2003	Controle de solicitação com data de início e conclusão
	Sanção por divulgar informações dos planos diferentes das constantes em certificado, regulamento ou contrato §2º, Artigo 10 da LC nº 109/2001 e §1º, da Res. CGPC nº 23/2006	Advertência ou multa Artigo 66 do Decreto nº 4.942/2003	Aprovação pelo gestor da informação, previamente à divulgação Política de Comunicação
	Nível inadequado de supervisão do fluxo de informações entre os vários níveis de gestão	Apontamentos por não atender o Artigo 7º da Res. CGPC nº 13/2004 Disponibilização de informações de forma indevida	Norma estabelecendo o nível de supervisão
	Não conseguir evidenciar as orientações/informações dadas por telefone	Reclamações e ou Processo Administrativo por não atender o participante/beneficiário	Utilização de sistemas de gravação para dirimir dúvidas

Quadro 7D

PROCESSO	FATOR DE RISCO	IMPACTO	CONTROLE
COMUNICAÇÃO	Disponibilizar informações restritas por anexar documentos indevidos em correio eletrônico	Perda financeira por divulgar informações restritas e risco de imagem	Rotina de verificação (abertura do documento) antes do envio
	Transmitir mensagem equivocada	Documento mal redigido pode gerar ônus à Entidade	Política de comunicação externa Apreciação prévia pela área de negócio e, quando couber, pelo jurídico
	Utilização de informações obtidas na rede internet sem os devidos cuidados	Possibilidade de responder processos caso a informação seja infundada	Normatizar a utilização de informações obtidas na rede internet
	Comentários inadequados em redes sociais (facebook, twiter e outros meios)	Leitor pode confundir posição/opinião pessoal com a Entidade	Política de utilização das redes sociais Acompanhar os comentários nas redes sociais
	Substituição de informação sem a devida comunicação	Utilização de informação obsoleta	Procedimento de substituição de informação formalizada, seja em que veículo for
	Artigos inadequados divulgados por terceiros	Risco de imagem	Conforme o caso gestão de crise, Política de Comunicação (autorização de divulgações) e Comitê de Conduta para apuração dos fatos
	Redação não conforme em relação ao aprovado	Pode acarretar vários riscos, desde o financeiro até o de imagem	Segregação de funções, com níveis de verificação, de acordo com o teor e registro do processo de aprovação
	Divulgação de informações indevidas ou equivocadas nos meios de comunicação, como o jornal	Criar passivos indevidos e perda de confiança	Passar por processo de aprovação, previamente normatizada

Quadro 7E

PROCESSO	FATOR DE RISCO	IMPACTO	CONTROLE
AUDITORIA E FISCALIZAÇÃO	Quebra de sigilo quanto às operações da Entidade e informações pessoais de participantes e assistidos, de que tiverem conhecimento em razão do cargo ou função	Divulgação indevida de informações Incorrer em falta grave, sujeitando o infrator à pena de demissão	No que ser refere à PREVIC não há controle A entidade deve controlar as informações e a quem foram disponibilizadas
	Deixar de atender à requisição de documentos ou de informação ou apresentar de forma deficiente ou incompleta	Auto de infração por não atendimento	Acompanhamento e validação pelo gestor da informação
	Deixar de encaminhar e/ou encaminhar informações inconsistentes	Sujeita a Entidade à visita técnica da ANS, conforme artigo 13 da Instrução Conjunta SPC/ANS Nº 01/2008 e comunicação à PREVIC	Política de comunicação Calendário de Obrigações
	Extravio de documentação	Sanções por perda de prazos	Gerenciamento de documento

Quadro 7F

A Comissão Técnica Nacional de Governança publicou em 2010, a 2ª edição do Manual de Controles Internos e, em 2011, o Livro Gestão Baseada em Riscos. Estas publicações trazem, com mais detalhes, conceitos e orientações para implementação de processos de gestão de riscos e controles, fundamental para garantir o perfeito funcionamento da EFPC, inclusive no que se refere à Segurança de Informações.

19. GERENCIAMENTO ELETRÔNICO DE DOCUMENTOS - GED

O aumento do volume de documentos, no decorrer do tempo, requer das entidades um controle mais eficaz, de forma a garantir uma correta guarda e acesso, e consequentemente uma maior segurança das informações.

O GED pode auxiliar no gerenciamento da documentação da entidade, seja ela física ou digital, de modo que o que ficava disperso em computadores, gavetas ou na cabeça das pessoas, possa ser controlado.

No GED é importante que se leve em consideração:

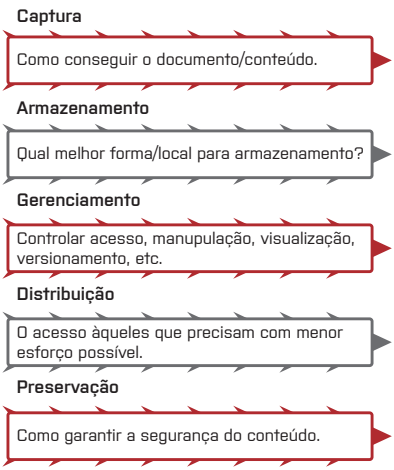


Figura 6

Um bom projeto de GED leva benefícios significativos a uma entidade, que são perceptíveis em praticamente todos os seus departamentos. Seguem alguns benefícios:

a) Extrema velocidade e precisão na localização de documentos;

b) Total controle no processo de negócio;

c) Ilimitadas possibilidades de indexação e localização de documentos;

d) Melhor qualidade no atendimento ao cliente. O GED proporciona respostas rápidas e precisas;

e) Mais agilidade em transações da Entidade;

f) Gerenciamento automatizado de processos, minimizando recursos humanos e aumentando a produtividade;

g) Melhoria no processo de tomada de decisões;

h) Maior velocidade na implementação de mudanças em processos;

i) Possibilidade de implementação de trabalho virtual, com redução de despesas;

j) Redução de custos com cópias, já que há disponibilização de documentos em rede;

k) Melhor aproveitamento de espaço físico;

l) Disponibilização instantânea de documentos (sem limitações físicas);

m) Evita extravio ou falsificação de documentos;

n) Agilidade em processos legais, nos quais é fundamental o cumprimento de prazos;

o) Aproveitamento da base de informática já instalada na empresa;

p) Integração com outros sistemas e tecnologias;

q) Tecnologia viabilizadora de outras, como ERP, SCM, CRM e BI;

r) Continuidade de negócios: o GED é de grande auxílio para políticas de recuperação de documentos e manutenção das atividades da empresa em casos de acidentes;

s) Facilitação às atividades que envolvem colaboração entre pessoas e equipes.

Como se pode observar o GED pode auxiliar na segurança de informação, garantido a integridade, confidencialidade, autenticidade e disponibilidade das informações, porém para que isto ocorra é importante que, ao se implantar tal sistema, se faça um adequado planejamento, envolvendo um grupo multidisciplinar, tratando da gestão de documentos da Entidade como um todo.

Faz parte do planejamento a identificação da demanda que será submetida ao GED, visualizando as vantagens que se pode obter utilizando essa tecnologia. Para isso, realiza-se um estudo para levantamento sobre o processo de criação de documentos, por meio de perguntas relevantes para a situação, tais como as sugeridas a seguir:

a) O que se deseja arquivar?

b) Onde são arquivados os documentos atualmente?

c) O que quer melhorar no sistema atual?

d) Quantas pessoas usam?

e) Quantas estações de trabalho existem?

f) Quantas pessoas serão afetadas?

g) Quais são as necessidades?

h) De onde vêm as informações?

i) Há aproveitamento de microfilme?

j) Natureza dos documentos em papel (formato, qualidade, padronização).

k) Quem arquiva?

l) Quem tem acesso?

m) Frequência de uso do arquivo?

n) Qual o formato dos registros no sistema atual?

Com as respostas a essas perguntas e a conclusão pela adesão/contratação do serviço de GED, os documentos são escaneados ou digitalizados em um processo de conversão de imagem digital, e, posteriormente, são submetidos a um processo de indexação, onde cada documento é nomeado e indexado através de informações obtidas dele mesmo. Só então, serão armazenados no banco de dados do sistema. Os documentos poderão ser lidos através da ferramenta de pesquisa e o administrador determinará por definicão de senha, quem terá acesso aos documentos.

Outro aspecto a se observar é a Legislação sobre o tema que é bastante ampla, pois engloba leis federais, estaduais e municipais, além da normatização específica por setor.

20. INFORMAÇÃO NA NUVEM

A nuvem se refere a locais na Internet, em que você pode salvar todo tipo de informação, incluindo fotos, músicas, documentos e vídeos, e recuperar facilmente esse material mais tarde usando um computador, telefone, TV ou outro dispositivo com conexão à Internet.

O interesse em torno da computação em nuvem se tornou muito grande. Muitos aclamam a computação em nuvem como um modo mais fácil e muito mais barato de prestar serviços de TI.

No setor de previdência, tem-se visto diversos relatos de EFPC que estão utilizando a nuvem. O importante é que, ao considerar a adoção de serviços de computação em nuvem, deve-se entender totalmente as implicações na segurança.

Quando usar a computação em nuvem, é importante saber onde os dados estão, como estão protegidos e quem pode acessá-los. Itens que devem ser detalhados pelos provedores de serviços de computação em nuvem e buscar do provedor a garantia de respeito à proteção de seus dados.

E, para entender e avaliar o tipo de segurança que o provedor de serviços de computação em nuvem oferece, é importante compreender os maiores riscos (Fonte: site da HP Hewlett Packard):

20.1. Os maiores riscos de segurança

a) Proteção de dados e gerenciamento de privacidade
Muitos provedores de serviços de computação em nuvem não oferecem acordos de nível de serviço (SLA). Isso significa que você fica sem garantia quanto à disponibilidade dos dados, privacidade ou proteção das informações.

b) Governança, risco e conformidade
Confiar seus dados a um provedor de serviços de computação em nuvem não significa que você está isento da responsabilidade de assegurar a proteção desses dados. A computação em nuvem aumenta riscos que alguns provedores de serviços podem não cuidar. Por exemplo, as políticas de retenção e registro de um provedor de serviços de computação em nuvem podem não atender às suas obrigações regulamentares. Se o provedor de serviços de computação

em nuvem não estiver fazendo o registro completo ou exato dos dados, você poderá ter problemas em uma auditoria de segurança.

c) Gerenciamento de identidades

Quando seus dados estiverem dentro do firewall do provedor de serviços, quem terá acesso a eles e em quais circunstâncias? Com que rapidez seu provedor de serviços pode conceder acesso? E, mais importante, com que rapidez ele cancela acesso administrativo e de usuário? Suas próprias políticas de autorização de dados podem ser excepcionalmente rígidas. Mas as políticas do seu provedor de serviços podem ficar fora do seu controle.

d) Segurança da infraestrutura

Os aplicativos e os dados confiados a um provedor de computação em nuvem ficam em servidores e armazenamento que você não escolheu ou que não mantém pessoalmente. A maioria dos fornecedores não dá visibilidade além de seus recursos virtuais. Então, como saber o nível de segurança que os equipamentos físicos realmente têm? Como saber se seus aplicativos estão sendo executados em um sistema operacional com *patches*[5] perfeitos e não em um repleto de buracos?

e) Preparação

Inserir, arbitrariamente, uma aplicação na computação em nuvem não é uma forma inteligente de avaliar a prontidão dela. No entanto, poucos provedores de serviços oferecem o tipo de avaliação necessária para definir se a aplicação faz sentido para a computação em nuvem.

f) Indisponibilidade do servidor

O seu fornecedor de nuvem pode perfeitamente sair do ar a qualquer momento. Isso pode acontecer com todos. Ser totalmente intacto às falhas de conexão não é um privilégio da computação em nuvem, assim como cremos que nunca será.

20.2. Como reduzir os riscos

A computação em nuvem não precisa ser repleta de riscos. Com o provedor de serviços certo, a computação em nuvem pode cumprir a promessa de serviços de TI mais flexíveis e mais fáceis de gerenciar,

5 *Patch* é um programa de computador criado para atualizar ou corrigir um software (fone:Wikipédia)

com preços mais acessíveis. No entanto, muito depende de seu preparo e de sua escolha dos provedores de serviços.

a) Classificação
Quando estiver pensando em serviços de computação em nuvem, primeiro classifique seus dados para determinar a adequação deles para a computação em nuvem. Uma parte importante desse processo é fazer uma análise do custo-benefício. As economias geradas quando se colocam os dados em nuvem compensam os riscos de brecha de segurança ou regulamentações de privacidade?

b) Avaliação
Encontre um provedor de serviços que faça avaliações de segurança para definir se os aplicativos ou os dados estão prontos para a computação em nuvem. Os melhores provedores de serviços irão determinar as regulamentações de conformidade às quais você está sujeito e irão ajudá-lo a cumprí-las.

c) Comece pelas informações não confidenciais
Não comece sua aventura pela computação em nuvem com aplicativos que exponham informações confidenciais de seus participantes. Comece por aplicações que ofereçam menos risco até você conseguir gerenciar com segurança o modelo e os serviços do seu provedor.

d) Avaliação crítica dos contratos do provedor de serviços
Descubra exatamente como o seu provedor de serviços pretende proteger seus dados e mantê-los privados na nuvem. Se os seus dados forem essenciais para os negócios, exija garantias satisfatórias do provedor. Isso inclui termos de serviço (TOS – *Terms of Service)* apropriados, políticas aceitáveis de uso (AUP – *Acceptable Use Policy*) e contratos de nível de serviços (SLA – *Service Level Agreement*).

e) Criptografia
Não deixe a criptografia para o seu provedor de serviços de computação em nuvem. Certifique-se de que você tenha um gerenciamento de ciclo de vida de chaves[6]. Além disso, usando a sua classificação de dados como orientação, faça a criptografia dos dados conforme apropriado e necessário.

6 Gerenciamento de chaves é o conjunto de técnicas e procedimentos que visa garantir a segurança das chaves. O comprometimento das chaves pode ocorrer de várias formas: as chaves podem ser capturadas, modificadas, corrompidas ou até mesmo disponilizada para pessoas não autorizadas, ou podem ser perdidas. O ciclo de vida de uma chave pode ser dividido em quatro fases: pré-operacional; operacional; pós-operacional; e de destruição.

f) Insista na transparência

Exija a capacidade de saber o que está acontecendo na infraestrutura física subjacente à infraestrutura virtual.

g) Recuperação de dados

Mesmo que você não saiba onde seus dados estão armazenados, um fornecedor de nuvem deve saber o que acontecerá com os dados e serviços em caso de algum desastre imprevisto, que possa vir a lhe comprometer de forma drástica, dependendo dos tipos de dados que armazenou na nuvem.

20.3. Conhecer é a melhor forma de prevenir

a) Acesso compartilhado

É comum os clientes compartilharem os mesmos recursos de computação: CPU, armazenamento, espaço, memória, etc., otimizando os recursos de infraestrutura e software. Tal modelo submete os clientes a riscos de (nossos) dados privados vazarem acidentalmente para outros inquilinos. Uma outra questão é que, na ocorrência de uma falha nesse compartilhamento, pode-se permitir que outro inquilino veja todos os dados ou assuma, inclusive, a identidade de outros clientes.

b) Vulnerabilidades virtuais

Cada provedor de serviços de nuvem é um enorme usuário de virtualização. E cada camada de virtualização representa uma importante plataforma na infraestrutura de TI, com vulnerabilidades embutidas que podem ser exploradas. Servidores virtuais estão sujeitos aos mesmos ataques que atingem os servidores físicos.

c) Autenticação, autorização e controle de acesso

Obviamente, os mecanismos de controle de autenticação, autorização e acesso do provedor de nuvem são fundamentais. Quantas vezes ele procura e remove contas obsoletas? Quantas contas privilegiadas podem acessar seus sistemas e seus dados? Que tipo de autenticação é necessária para os usuários privilegiados? A sua empresa compartilha um espaço comum com outros inquilinos?

Certifique-se que os prestadores dos serviços de computação na nuvem limitam o acesso dos funcionários e as autorizações ao estritamente necessário para a realização de sua tarefa.

Proteção de dados é outra grande preocupação. Se a criptografia de dados é usada e aplicada, as chaves privadas são compartilhadas entre os inquilinos? Quem e quantas pessoas na equipe do fornecedor de nuvem podem ver os seus dados? Onde os seus dados estão armazenados fisicamente? Como seu dado é tratado quando deixa de ser necessário?

d) Disponibilidade

Quando você é um cliente de um provedor de nuvem pública, redundância e tolerância a falhas não estão sob seu controle.

O fornecedor de nuvem geralmente afirma fazer *backups* dos dados dos clientes. Mas, mesmo com os *backups* garantidos, a risco de perda de dados - e de forma permanente. Se possível, a entidade deve sempre fazer o *backup* dos dados compartilhados na nuvem por conta própria. Ou se resguardar, em contrato, estabelecendo as responsabilidades do provedor por perdas de dados.

Alguns provedores de computação na nuvem dependem de terceiros para prestar determinados serviços. A EFPC precisa saber identificar as interdependências potencialmente problemáticas. Considere um modelo de governança em que um fornecedor detém a responsabilidade global para as interrupções e as falhas de segurança.

e) Posse

Esse risco é quase sempre uma surpresa para os clientes de nuvem, mas, muitas vezes, eles não são os únicos proprietários dos dados. Muitos provedores de nuvem pública, incluindo os maiores e mais conhecidos, possuem cláusulas em seus contratos que afirmam explicitamente que os dados armazenados pertencem a ele provedores - e não ao cliente.

Há conhecimento de casos nos quais o fornecedor de nuvem saiu do negócio e, em seguida, vendeu os dados confidenciais dos clientes como parte de seus ativos. Certifique-se de que você tem esse risco previsto em seu contrato e, de alguma forma mitigado. Deixe claro quem é o dono dos seus dados e o que o fornecedor de nuvem pode fazer com eles.

Mesmo quando os riscos de computação em nuvem são conhecidos, eles são difíceis de calcular com precisão real. Não há histórico suficiente para determinar a probabilidade de falhas de segurança ou disponibilidade, especialmente para um determinado fornecedor, ou se

esses riscos vão levar a danos substanciais para os clientes.

Estabeleça o melhor que puder as responsabilidades do fornecedor de nuvem. Só fazendo as perguntas difíceis você poderá começar a entender os riscos totais da computação em nuvem pública.

É preciso analisar detalhadamente as opções para proteção de dados sensíveis oferecidas pelos provedores de serviços de computação na nuvem. O quanto fluem através da rede, o quanto residem em um servidor, ou na infraestrutura de armazenamento.

Para começar, peça aos fornecedores informações sobre o uso de VPNs, o gerenciamento de chaves, e as opções de criptografia. Antes de assinar um contrato, examine os termos relativos à privacidade de dados, como serão auditados, a confiabilidade do serviço, e contingências contra alterações.

Por fim, certifique-se de elaborar uma estratégia de mitigação de risco de modo que você seja capaz de migrar o seu trabalho para um novo provedor (ou voltar a mantê-lo *in house*) com rapidez e facilidade em caso de uma eventualidade.

É importante que se tenha consciência de que a proteção dos dados armazenados em nuvem também depende dos usuários que devem proteger suas senhas e seus computadores.

21. PAPEL DA COMUNICAÇÃO

> A comunicação e divulgação de informações a conselheiros, patrocinadores, instituidores e participantes deve ser feita em linguagem clara e direta, utilizando-se os meios adequados, assim entendidos aqueles que, inequivocamente, cumpram tal objetivo, observada a racionalidade, em termos de custos e métodos, com informações sobre as políticas de investimentos, as premissas atuariais, a situação econômica e financeira, bem como os custos incorridos na administração dos planos de benefícios. A EFPC deve informar, ainda, sempre que solicitada pelos interessados, a situação de cada participante ou assistido perante seu plano de benefícios.
>
> A comunicação clara e tempestiva entre a EFPC e os participantes e assistidos deve ser incentivada por todos os meios. É recomendável a implementação de um canal de comunicação, pois este constitui importante instrumento para o aprimoramento do processo de transparência na gestão da entidade.
>
> É recomendável a utilização da rede mundial de computadores e de outras tecnologias, para dar agilidade na difusão das informações aos participantes e assistidos.

Guia PREVIC

As políticas de Comunicação têm essencial papel na gestão da informação sendo fundamental que nela sejam contemplados cuidados que vão desde o dimensionamento e detalhamento da demanda (se é realmente necessária, qual a prioridade, o que dizer e para quem, por quê, quando, etc.) até a correção e atualidade das informações.

A EFPC tem como dever utilizar uma linguagem simples e clara em seu relacionamento com participante, daí a necessidade de envolver os especialistas de comunicação na tarefa de informar, porém, deve ser acompanhado, em todas as etapas de produção, pelos setores demandantes, cabendo-lhe revisar o conteúdo para garantir que a abordagem das informações não tenha seu sentido alterado.

A Comissão Técnica Nacional de Comunicação da Abrapp, em seu guia sobre política de comunicação nas EFPC, descreve a importância de que não se desenvolvam ações isoladas nas criações de cartilhas e programas, de forma a assegurar a qualidade das informações, que não se resume apenas ao conteúdo.

A comunicação tem suas sutilezas que só profissionais da área dominam e qualquer ação equivocada pode provocar graves prejuízos, especialmente, nos tempos atuais, com a tendência de comunicação com os participantes, utilizando o celular (SMS) e a internet, e ferramentas de interação como redes sociais e e-mails, ao mesmo tempo em que pode agilizar e ampliar o fluxo de informações, traz preocupações com relação à sua correta utilização e outras vulnerabilidades.

Para mitigar os riscos de utilização inadequada dos canais de comunicação é recomendável adotar algumas práticas:

a) Estabelecer normas específicas para uso das Redes Sociais disponíveis na rede mundial de computadores (Internet), de modo a evitar o mau uso, o que pode materializar, dentre outros, o risco de perda financeira e risco de imagem para a entidade;

b) Quando a organização enfrenta uma crise, a sua reputação está em risco. Nesse momento, a comunicação é uma das ferramentas mais importantes para proteger os interesses das entidades e conduzi-las de volta à normalidade. A área de comunicação atuará sobre a percepção de diversos públicos (imprensa, funcionários, órgãos públicos, sindicatos, participantes, entre outros) através de mensagens direcionadas, sejam de ataque ou de defesa. A maneira mais eficaz, no entanto, de proteger-se de uma crise é o planejamento prévio, por meio de um diagnóstico dos riscos relativos à entidade e ao setor, traçando procedimentos para cada situação, estabelecendo quem faz o que, como e quando. Os dirigentes devem ser treinados para saberem executar suas funções caso enfrentem uma crise. Os procedimentos se dividem em três fases: antes, durante e após a crise.

c) A comunicação interna existe sempre, mesmo que nunca tenha sido definida uma política. As conversas de corredores ou durante a pausa para café são um espaço privilegiado para a comunicação interna. A diferença é que uma política de comunicação interna é uma forma eficaz de combater rumores, estimular o envolvimento dos seus empregados nos projetos da empresa e instaurar um clima de confiança.

d) As informações devem fluir com clareza e transparência dentro das Entidades. Pessoas bem informadas conscientes do processo no qual participam, produzem mais, criam menos problemas e permanecem motivadas. Além disso, o processo de comunicação deve garantir que as informações cheguem até seus destinatários sem perder seu conteúdo, pois um pequeno desvio de informação pode acarretar em prejuízos imensos, de dinheiro e tempo.

e) Implementar Política de Comunicação com objetivo de promover a comunicação da entidade com seus públicos de relacionamento, de forma coordenada e sinérgica. O documento indicará os processos para o fluxo de trabalho da comunicação: gestão da comunicação, gestão de conteúdo, comunicação interna, relação com a imprensa, comunicação institucional e comunicação com a comunidade.

22. CONSIDERAÇÕES FINAIS

Como citado neste trabalho, há um grande volume de informações sendo geradas nas entidades e, dada a crescente evolução da tecnologia, estas circulam em grande velocidade. Paralelamente a isso, o acesso a elas, quase que imediato, se torna uma exigência por parte dos interessados, seja pela internet, por meio de smartphones, documentos físicos, entre outros. Fato é que não se vislumbra um retrocesso neste cenário e, assim sendo, as Entidades devem se atentar a essas evoluções e estabelecer procedimentos e controles que minimizem a materialização de riscos à sua segurança.

Nosso sistema é composto por entidades de portes e complexidades diversas, contudo, na essência, a responsabilidade sobre as informações é a mesma.

Desta forma, nenhuma delas pode se eximir de estabelecer controles que reduzam os riscos de uma informação ser acessada por pessoas não autorizadas, ser extraviada ou alterada ou, ainda, não estar disponível tempestivamente.

Assim, o principal objetivo desta Comissão Técnica foi sensibilizar as entidades e seus dirigentes sobre a necessidade de avaliar constantemente os riscos à segurança da informação em todos os processos, por meio de discussão em grupos multifuncionais, e minimizá-los implementando controles para garantir a correta disponibilização e acesso.

É importante destacar que a segurança da informação há muito deixou de ser uma preocupação das áreas de TI das entidades, passando a ser um fator de risco presente em qualquer área operacional ou de negócio.

Por esse motivo, as ações de mitigação dos riscos em segurança da informação devem ser endossadas e patrocinadas pela alta administração da entidade, por meio da adoção de políticas e procedimentos específicos, campanhas educativas de esclarecimento e conscientização dos colaboradores.

O assunto não se esgota aqui e exige permanente acompanhamento de modo a se avaliar as novas ameaças e vulnerabilidades e definir medidas necessárias à preservação da informação de nossos participantes e entidade.

REFERÊNCIAS

O Manual de Governança em Segurança da Informação foi elaborado a partir de experiências profissionais e acadêmicas dos membros da Comissão Técnica Nacional de Governança, das Comissões Técnicas Regionais Centro Norte e Sul de Governança e de consultas às seguintes fontes:

- FONTES, Edison. Praticando a Segurança da Informação. BRASPORT, 2008
- Constituição Federal 1988
- Leis Complementares nºs 108 e 109/2001
- Resolução CGPC nº 13, 1º de outubro de 2004
- Plano de Continuidade de Negócios da REGIUS - Sociedade Civil de Previdência Privada, 29 de dezembro de 2010
- Diretriz Executiva de Gestão da Segurança da Informação da Fundação dos Economiários Federais – FUNCEF, 14 de abril de 2010
- Revista do 31º Congresso Brasileiro dos Fundos de Pensão, novembro de 2010
- NBR ISO 27001
- Artigo do XVIII Encontro Nacional da Engenharia de Produção
- Site: www.fabiovaz.com.br
- Site: www.pwc.com.br/pt_BR/br/publicacoes
- Site:http://h71028.www7.hp.com/enterprise/w1/pt/messaging/feature-enterprise-cloud-security.html
- Capítulo 17 – Considerações quanto à Segurança na Computação na Nuvem, do Livro Certificação Security+ (www. editoranovaterra.com.br)
- GED – Gerenciamento Eletrônico de Documentos a tecnologia que está mudando o mundo

COMISSÃO TÉCNICA NACIONAL DE GOVERNANÇA

Diretor
Milton Luís de Araújo Leobons (PRECE)

Coordenadora
Adriana de Carvalho Vieira (OABPREV-SP)

Membros
Adriana Barreto Rodrigues (ELETROS)
Antonio Carlos Bastos D'Almeida (FORLUZ)
Benilton Couto da Cunha (ECONOMUS)
Décio Magno Andrade Stochiero (SISTEL)
Gema de Jesus Ribeiro Martins (PETROS)
Herbert de Souza Andrade (FUNDAÇÃO ITAÚSA INDUSTRIAL)
José Roque Fagundes da Silva (FACHESF)
Karina Damião Hirano (SP-PREVCOM)
Luiza Miyoko Noda (FUNDAÇÃO COPEL)
Marcelo Coelho de Souza (PREVI)
Mariana de Azevedo Mitzakoff (HSBC FUNDO DE PENSÃO)
Mary Stela Kloster (FIBRA)
Max Mauran Pantoja da Costa (FUNCEF)
Miriam Garrido Pacheco Leite (ICATU FMP)
Nilceia Stopa Mendes (METRUS)
Nilton Akira Yamamoto (FUNDAÇÃO CESP)
Rosângela Palhares Sales Jardim (MULTIPREV)
Silvio Gulias Junior (POSTALIS)

COMISSÃO TÉCNICA REGIONAL CENTRO-NORTE DE GOVERNANÇA

Coordenador (Interino)
Fábio Ricardo Motta de La Plata (POSTALIS)

Membros
André Luis Sales da Silva (ELETRA)
Arilson Matos Gonçalves (CENTRUS)
Christiano Augusto Gomes Fernandes (SISTEL)
Felizana Maria Maia da Silveira Palhano (ENERSUL)
Jamile Ribeiro Macedo Monteiro (FACEB)
Kátia Bezerra Rodrigues (PREVINORTE)
Max Mauran Pantoja da Costa (FUNCEF)
Semíramis Rezende e Silva Magalhães Cézar (REGIUS)
Wenceslau J Goedert (CERES)

COMISSÃO TÉCNICA REGIONAL SUL DE GOVERNANÇA

Coordenadora
Luiza Miyoko Noda (FUNDAÇÃO COPEL)

Membros
Adriana Nobre Nunes (ELETROCEEE)
André Campestrini Gomes (BOTICÁRIO PREV)
Diclô Espedito Vieira (PREVUNISUL)
Élcio Nóbrega Junior (ELOS)
Emerson Roberto Leska (FUSAN)
Esttela Maria Berri (FUNDAÇÃO COPEL)
Luana Celina de Deus (FUNCORSAN)
Lucimary Bondi Sartori (FUNBEP)
Renata de Paula Rodrigues Pereira (CELOS)

Estendemos nossos agradecimentos a todos que passaram pela Comissão Nacional de Governança, dando valiosas contribuições para a realização deste projeto, em especial Srs. Acyr Xavier Moreira (PREVI), Antônio Bráulio de Carvalho (FUNCEF), Luiz Ricardo da Câmara Lima (FACHESF), Paulo Leite Julião (ECONOMUS), Robson Candido da Silva (VALIA) e Denise Ornellas (MULTIPREV).

Abrapp - Associação Brasileira das Entidades Fechadas de Previdência Complementar
www.portaldosfundosdepensao.org.br
Tel.: (11) 3043.8777
Fax: (11) 3043.8778/3043.8780
Av. das Nações Unidas, 12551 – 20° andar – Brooklin Novo
04578-903 – São Paulo – SP
www.abrapp.org.br
www.facebook.com/abrapp

ABRAPP

ISBN 978-85-99388-37-2
9 788599 388372