RELATÓRIO DE METAS ESTRATÉGICAS – 2013

O presente relatório visa apresentar à Administração do TRE os avanços dos trabalhos da Comissão de Segurança de Informação, em especial o cumprimento da meta de 2013.

À DG/ASSESD.

Em 18.02.2014

Arthur Ribeiro Rocha
SGP

Geraldo Majella Nunes de Moura
SCI

Milena de Jesus Sousa
Corregedoria

Najara Andrade Guimarães Carneiro
DG

Paulo de Campos Vieira
ASCOM (Suplente)

Rilson Barros de Almeida
STI (Presidente)

Sidney Santos Doria
STI (Vice-Presidente)

Vítor Marcelo Pinto Soares
ZE (Suplente)

William Deivis do Nascimento Pereira
SEGIN

1. Introdução (Histórico)

No estágio atual de globalização dos mercados mundiais observa-se uma tendência crescente das corporações em destacar e priorizar os projetos voltados a gestão, com o objetivo de aumentar a eficiência dos negócios. De forma similar, os governos têm investido em gestão pública, visando atender à necessidade crescente de competitividade que as nações precisam alcançar para manterem seus níveis de desenvolvimento, adaptando-se a tais mercados globalizados.

Nesse contexto, a elaboração de diretrizes, planos e ações voltadas à gestão pública são cada vez mais comuns em todas as esferas do Estado Brasileiro. Para assegurar a continuidade e a eficiência dos processos governamentais, os órgãos de controle brasileiros, nas três esferas de poder, têm recomendado que os órgãos da administração direta invistam na segurança das infraestruturas críticas da informação, sejam elas informações em processos, pessoas ou até instalações físicas especiais. Relativos à segurança da informação, destacam-se a crescente convergência tecnológica, a elevada interconexão de redes e sistemas, e sua interdependência.

Para que cada unidade administrativa entenda o valor da implantação de uma Política de Segurança da Informação (PSI), é necessário compreender que não se trata apenas de um documento, cujo valor nasce na data de sua publicação. O produto mais importante que resulta da implantação de uma PSI não é o documento em si, que terá o papel de marco e de memória, mas a transformação que ocorre em cada área interna, ao longo do processo.

É exatamente quando cada área precisa verificar as informações com que lida, o valor de cada informação, o quão vulneráveis tais informações estão, é nesse momento que se cria o desejo interno de modificar os processos da área, tendo como alvo a continuidade do negócio público. A PSI em si resta como subproduto natural dessas mudanças positivas, sua formalização.

No intuito de implantar a sua Política de Segurança da Informação, o Tribunal Regional Eleitoral da Bahia partiu com duas ações estratégicas: (i) a inclusão da meta *Implantação da Política de Segurança da Informação* em seu plano estratégico plurianual e (ii) a criação da *Comissão de Segurança da Informação* (CSI), composta de integrantes de diversas áreas e responsável por tomar as medidas necessárias para o cumprimento dessa meta estratégica, no prazo definido. Tais ações estão em consonância com a Res. TSE 22.780/2010 e com recomendações expressas do CNJ e do TCU.

Com a CSI instituída, a primeira providência tomada por esta comissão foi se capacitar sobre segurança da informação. Em seguida, sob a orientação da Res. TSE 22.780/2010, foram definidas as metas plurianuais para a implantação da Política de Segurança da Informação, associadas ao Plano Estratégico do TRE-BA. A meta estabelecida para 2012 foi *Realizar um Plano Piloto de Levantamento de Ativos da Informação na CODEPS,* e, para 2013, o desafio foi ***estender este levantamento a todas as unidades do Tribunal*.**

O levantamento de ativos da informação é a primeira fase para a implantação de uma PSI, onde os ativos de informação são elencados e associados formalmente aos seus respectivos

responsáveis. Entretanto, esta pode ser uma tarefa difícil, visto que será o primeiro contato das áreas do Tribunal com os conceitos formais de Segurança da Informação. Por isso, a primeira meta da CSI foi a realização de um plano piloto de levantamento de ativos da informação que visou, primordialmente, treinar as áreas envolvidas e a CSI nesta tarefa.

O plano piloto foi realizado formalmente, baseado na metodologia de Levantamento de Ativos da Informação da Universidade Cernegie Mellon (STEVENS, 2005), seguindo a metodologia descrita no Anexo III.

2. Levantamento de Ativos da Informação - 2013

Resumidamente, o trabalho da CSI foi procurar uma maneira de divulgar o questionário utilizado no plano piloto realizado em 2012 de forma segura e rápida a todas as unidades do Tribunal. Para tanto, foi escolhido o software para aplicação de questionários *online* "*LimeSurvey"*, já utilizado pela COELE (Coordenadoria de Eleições), por tratar-se de uma ferramenta *free,* de fácil operação, acessível pela *intranet* e possibilitando o acesso personalizado, através de senhas (*tokens*) geradas e disponibilizadas aos servidores responsáveis por responder ao questionário proposto.

O levantamento foi então determinado pela Ordem de Serviço nº 08/2013 (Expediente 81.870/2013), a qual fixou o prazo de 11 de novembro a 02 de dezembro para que os responsáveis previamente designados pelos gestores de suas respectivas áreas procedessem à atividade em tela.

Por se tratar de algo novo, uma das maiores dificuldades enfrentadas foi vencer a resistência, em especial dos servidores das zonas eleitorais, quanto às seguintes questões:

"o que é um ativo de informação ?";
"é realmente necessário responder ao questionário ? (não sou da área de TI)";
"os ativos característicos das zonas eleitorais não são os mesmos ? por que devo responder, se são praticamente iguais ?";
"o prazo está muito apertado, não sei se conseguirei responder a tempo"

Muitas destas dúvidas puderam ser dirimidas por meio de apresentação realizada no auditório do Tribunal na data de 25.11.2013, onde foram dadas instruções para a realização do levantamento de ativos; adicionalmente, visando alcançar também os colegas do interior, foi criada a página da CSI na intranet, contendo as instruções necessárias para a realização da atividade.

Outras questões que merecem ser pontuadas dizem respeito:

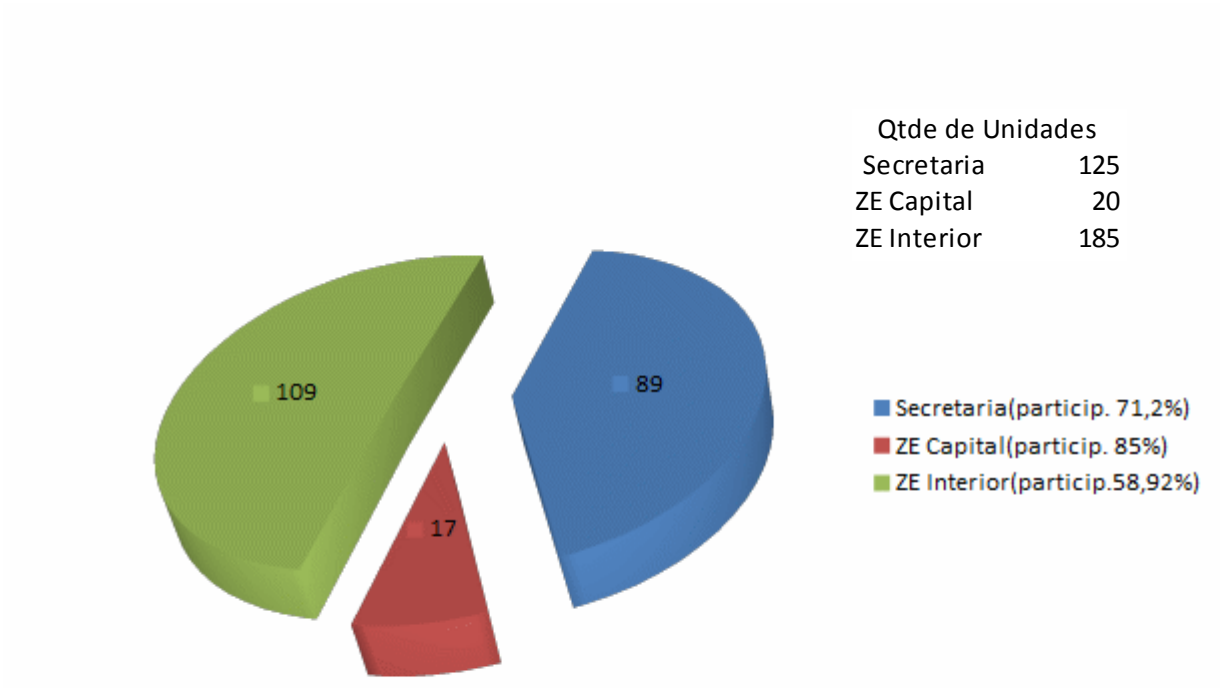
a) ao tamanho reduzido da Comissão (7 membros), sendo que, por motivo de férias/afastamentos/licenças, efetivamente apenas 3 mantiveram-se envolvidos na tarefa proposta;

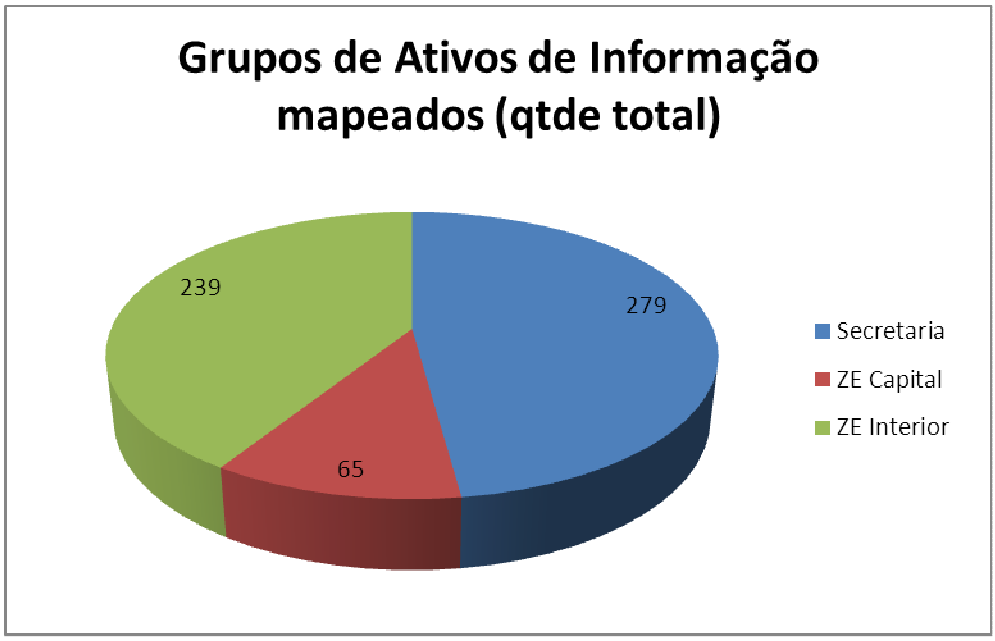
b) o período da realização da atividade não foi o mais adequado – final do ano, quando alguns titulares das unidades não estavam em efetivo exercício.

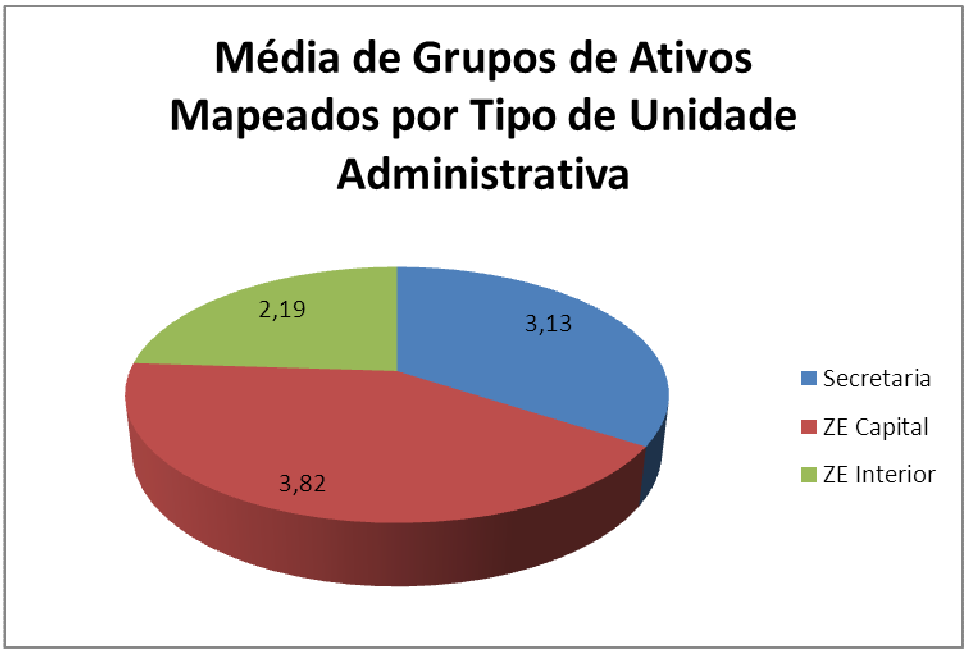
3. Consolidação das Respostas

Com relação às unidades envolvidas no levantamento, foi registrada participação global superior a 65% - o equivalente a 215 respostas do universo de 330 unidades envolvidas. No total, foram respondidos 583 questionários, correspondentes aos grupos de ativos mapeados pelas unidades, com a participação expressiva de 71,20% (89/125) das unidades da Secretaria e 61,46% (126/205) dos Cartórios Eleitorais (incluídas as zonas da capital e interior), conforme gráficos a seguir:

Participação por Unidade Administrativa
(total: 330)




Grupos de Ativos de Informação mapeados (qtde total)
239
279
65
Secretaria
ZE Capital
ZE Interior


Média de Grupos de Ativos Mapeados por Tipo de Unidade Administrativa
2,19
3,13
3,82
Secretaria
ZE Capital
ZE Interior

4. Observações

Como primeiro passo, e para muitos, o primeiro contato com o tema "Segurança da Informação", a CSI classificou a atividade como uma experiência válida, e que servirá de insumo para os próximos passos:

a) classificação das informações ora mapeadas, além de sistemas e equipamentos, quanto à necessidade de sigilo, confidencialidade e disponibilidade;

b) novo ciclo de levantamento de ativos, quando espera-se que os servidores tenham maior maturidade quanto aos aspectos da segurança da informação. Ressalte-se que, por tratar-se de um processo iterativo, que periodicamente deve ser revisado (em decorrência de mudanças no ambiente, novas ameaças/tecnologias/serviços que potencialmente venham a comprometer a segurança dos ativos), a CSI sugere que um novo ciclo de levantamento de ativos seja realizado no **primeiro trimestre de 2015** (por tratar-se de ano não-eleitoral, bem como evitar a realização da atividade próxima ao final do ano) ;

c) contratação de consultoria externa para realizar a Análise de Riscos, Elaboração do PDTI e PCN (*Disaster Recovery*). Como a CSI não possui o *expertise* necessário para realizar estas atividades, e também não dispõe de orçamento próprio, foi feita a solicitação à Diretoria-Geral, por meio do Expediente 92.295/2013, o qual encontra-se, nesta data, aguardando a inclusão dos respectivos recursos no Plano Anual de Contratações para o exercício de 2015 (PLANCONT 2015).

5. Respostas dos Questionários

Por uma questão de economia, as respostas não serão impressas. Para visualizá-las, acesse o link abaixo (Anexo I):

http://intranet.tre-ba.gov.br/institucional/comissoes/seguranca-da-informacao/respostas_LAI_2013_PDF.pdf

ANEXO II

RELATÓRIO DE ATIVIDADES – CSI - 2013

1. elaboração de página da CSI na intranet do TRE-BA (http://intranet.tre-ba.gov.br/institucional/comissoes/seguranca-da-informacao);

2. levantamento de ativos da informação em todas as unidades do Tribunal, em cumprimento à meta estabelecida pela Diretoria-Geral; este levantamento foi determinado pela Ordem de Serviço nº 08/2013 (Expediente 81.870/2013) e servirá de base para a análise de riscos associados aos itens mapeados;

3. solicitação de recursos (Expediente 92.295/2013) para garantir a contratação, a partir do exercício de 2015, de consultoria externa para a realização de:
   i) processo de classificação das informações, sistemas e equipamentos do Tribunal;
   ii) plano formal de gestão de riscos de Segurança da Informação;
   iii) Plano de Continuidade de Negócios (PCN);
   iv) Plano Diretor de TI (PDTI), a ser desenvolvido em parceria com a STI, em conformidade com o PETI (Planejamento Estratégico de TIC).

4. divulgação da política de segurança da informação do TSE, ora adotada pelo TRE-BA até a elaboração de norma própria. Realizada através da página da CSI, matéria da ASCOM e e-mail encaminhado a todos os servidores, além de evento realizado no auditório em 25.11.2013 (instruções para a realização do levantamento de ativos);

5. elaboração, em conjunto com a STI, das seguintes normas de segurança da informação (NSI):
   NSI-01 - Política de Backup de Dados Corporativos - Portaria 796/2013 da Presidência, publicada no DJE de 30.09.2013
   NSI-02 - Instituição no âmbito da Justiça Eleitoral da Bahia do papel de Gestor de Sistema (Expediente 87.426/2013).

6. participação do servidor Rilson Almeida, na qualidade de Presidente da CSI, do evento "Seminário de Segurança da Informação - Estados", promovido pelo TCU nos dias 11 e 12 de novembro de 2013, na modalidade de videoconferência.

ANEXO III

Metodologia utilizada para o Levantamento de Ativos da Informação (Plano Piloto em 2012)

3.1. **Visão Geral**

Segundo a ABNT (2005), Segurança da Informação (SI), como parte integrante do processo global de Gestão de Segurança, tem como objetivo proteger a informação contra ameaças no intuito de garantir a continuidade, minimizar os danos e maximizar os investimentos e oportunidades do negócio. A segurança da informação é obtida com a utilização de controles: políticas, práticas, procedimentos, estruturas organizacionais e infra-estruturas de *hardware* e *software*. É caracterizada pela preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação, e visa preservar nas empresas a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais.

Para que uma organização identifique seus requisitos de segurança, ela deve basear-se em três pilares. O primeiro é o conjunto dos princípios, objetivos e necessidades para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações. O segundo é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender. E o terceiro, oriunda das duas anteriores, são os requisitos de segurança derivados da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos ao negócio.

Em tese todas as atividades de uma organização envolvem risco. As organizações que gerenciam o risco buscam identificar, analisar, avaliar e tratar os riscos identificados, a fim de atender aos critérios e requisitos necessários à continuidade de suas operações.

A Gestão de Riscos (GR) quando implantada e mantida possibilita:

a) Aumentar a probabilidade de atingir seus objetivos;

b) Encorajar a gestão pró-ativa;

c) Identificar e tratar os riscos através de todo o Tribunal;

d) Melhorar a governança;

e) Melhorar os controles;

f) Melhorar a eficácia e eficiência operacional;

g) Minimizar perdas;

h) Aumentar a resiliência da prestação de serviços do Tribunal.

Definir o escopo de aplicação da Gestão de Riscos de Segurança da Informação é, portanto, necessário a fim de delimitar seu âmbito de atuação. Esse escopo pode abranger o Tribunal como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação.

De forma simplificada as ameaças à segurança da informação se concentram em dois pontos: as vulnerabilidades existentes nos ambientes onde a informação é processada, armazenada ou transmitida e as ameaças externas e internas à segurança da informação nestes ambientes. É importante compreender aqui que armazenamento, processamento e transmissão são verbos que podem sugerir informações digitais, mas na verdade eles valem para um documento em papel, em que, por exemplo, um processamento poderia ser a adição de um parecer baseado nas informações antes contidas no papel. Independentemente destas definições entende-se que uma Gestão de Riscos de Segurança da Informação deve contemplar as seguintes ameaças potenciais:

a) Terremotos	j) Incêndios
b) Furacões ou Tornados	k) Contaminação Química
c) Inundação	l) Distúrbios Sociais
d) Falta de Energia	m) Bombas
e) Problemas no Transporte Público	n) Terrorismo
f) Greves	o) Falhas de *Hardware*
g) Pandemias	p) Falhas de *Software*
h) Escândalos	q) Vírus e *Worms*
i) Vazamento de Informações	r) Morte de Pessoa-Chave

Ademais, deve-se compreender que a Gestão de Riscos tem caráter preventivo e por isso os riscos sempre existirão, por mais que se empreguem esforços para minimizá-los. Assim, a idéia aqui é manter o bom senso para permitir a operacionalização da segurança, considerando:

a) O escopo do que se vai manter sob o risco gerido, contendo tudo o que deve ser gerenciado e nada a mais. O que estiver fora do escopo é considerado risco assumido. Assuma que sempre haverá riscos assumidos num plano de Gestão de Riscos;

b) Planos de proteção que sejam compatíveis com o valor (mesmo que imaterial) dos ativos e com o risco associado ao ativo;

c) Gestão de Riscos, assim como a Gestão de Segurança da Informação é um processo iterativo e evolutivo. Não há o plano perfeito na primeira vez. Não há listagem de ativos da informação completa na primeira vez e assim por diante.

Por fim, para que um ativo de informação esteja protegido de forma adequada é necessário que se identifiquem as ameaças potenciais e os possíveis impactos aos seus ativos, processos ou pessoas, caso estas ameaças se concretizem. Mesmo ativos da informação já identificados e

protegidos podem sofrer sinistros. Neste caso, entra em ação o Plano de Continuidade de Negócios, que será produzido em outra etapa e também está previsto como meta do TRE-BA.

3.2. **Macro-Processos**

O Levantamento de Ativos de Informação é um processo iterativo e evolutivo, em três etapas: (i) identificação e classificação de ativos de informação, (ii) identificação de potenciais ameaças e vulnerabilidades e (iii) avaliação de riscos.

O produto de cada atividade servirá de insumo para as atividades subseqüentes, e o resultado final do processo deverá proporcionar à Administração condições para priorizar quais ativos de informação deverão receber ações de controle, visando o tratamento de riscos para a redução dos impactos ao negócio público. Além disso, o produto final do processo irá subsidiar as atividades de identificação e classificação de ativos de informação e identificação de potenciais ameaças e vulnerabilidades quando o novo ciclo do processo for executado.

3.2.1. Identificação e Classificação de Ativos da Informação

O crescente incremento da complexidade técnica e ambiental dos negócios representa grandes obstáculos e desafios para aqueles que necessitam proteger seus ativos de informação. Esses ativos, por sua vez, sofrem constantes processamentos e combinações, gerando outros recursos cada vez mais complexos e inter-relacionados. É tênue a linha entre posse e custódia dos recursos de informação, pois a informação flui livremente por toda a organização e frequentemente ultrapassa suas fronteiras chegando a outros participantes, como: colaboradores, clientes, fornecedores e concorrentes. O processo de Identificação e Classificação de Ativos de Informação auxilia a organização a conhecer, valorizar, proteger e manter seus recursos em conformidade com os requisitos legais e do negócio.

De forma geral, o processo de Identificação e Classificação de Ativos de Informação tem como objetivos prover a uma organização: (i) um entendimento comum, consistente e inequívoco das fronteiras dos ativos, (ii) a identificação clara de seu(s) responsável(is), (iii) um conjunto completo de informações sobre os requisitos de segurança de cada recurso, (iv) uma descrição de onde o bem está contido, é processado e é transportado e (v) a identificação do valor que o ativo representa para o negócio. Por fim, o processo cria condições para que se possa desenvolver e aplicar planos de gerenciamento de riscos sobre tais ativos.

O processo de Identificação e Classificação de Ativos de Informação no TRE-BA será composto por seis atividades:

1. Coletar informações gerais;
2. Definir as informações dos ativos;
3. Identificar o(s) responsável(is);
4. Identificar os contêineres dos ativos;
5. Definir os requisitos de segurança;

6. Estabelecer o valor do ativo de informação.

Cada atividade do processo coleta informações adicionais sobre os recursos, as quais podem ser refinadas conforme novas percepções identificadas nas atividades seguintes. Quando isto acontece, o processo dever ser reiniciado com cada ativo de informação para garantir precisão e a consistência entre as atividades.

3.2.2. Atividade 1 – Coletar Informações Gerais

O objetivo desta atividade é definir como será a estratégia da coleta das informações, quem serão os responsáveis e qual a previsão de conclusão dos trabalhos.

É natural que os recursos da informação evoluam com o tempo; desta maneira, os perfis gerados pelo mapeamento dos ativos da informação precisam ser constantemente atualizados ou até mesmo recriados. Além disto, pode ser necessário investigar ou saber a história de um ativo.

3.2.3. Atividade 2 – Definir as Informações dos Ativos

A finalidade desta etapa é caracterizar o escopo da atividade de mapeamento, ou seja, antes de se executar qualquer tarefa, a organização deve compreender e concordar sobre quais ativos serão considerados e qual o nível de profundidade das informações coletadas.

O nível de detalhe das informações dos ativos, definido pela organização, deve ser suficiente para determinar o conteúdo do recurso, suas fronteiras, o(s) responsável(is), o valor e os requisitos de segurança.

Deve-se utilizar o bom senso e ser consistente na definição dos ativos para ajudar a reduzir a complexidade na coleta das informações.

A definição do recurso da informação deve esforçar-se para satisfazer exigências mínimas de:

- **Consistência** (i.e., não muda durante curtos períodos de tempo);
- **Clareza** (i.e., não é ambígua ou vaga, sujeitando a dupla interpretação);
- **Entendimento universal** (i.e., está acima de linguagens e tecnologias);
- **Aceitação** (i.e., é aceitável conforme requisitos do negócio);
- **Materialidade** (i.e., é clara a respeito de como o recurso se apresenta - papel, mídia magnética, etc.).

É importante, quando possível, envolver o responsável pelo recurso e outras partes interessadas no processo da definição. Isso assegurará a exatidão e a consistência da definição e da aceitação da atividade. Em alguns casos o responsável não poderá ser determinado até que o recurso seja totalmente definido. Nestes casos, a definição do recurso da informação deve ser revista com o responsável após este ser identificado na **Atividade 3**.

3.2.4. Atividade 3 – Identificar o(s) Responsável(is)

O responsável por um ativo de informação deve ser uma parte interessada da organização, legalmente instituído, responsável por:

- Descrever o recurso da informação, conforme atividade 2;
- Definir as exigências de segurança do recurso da informação, conforme atividade 5;
- Comunicar as exigências de segurança do recurso da informação a todos os usuários;
- Assegurar-se de que as exigências da segurança estejam cumpridas através de monitoramento;
- Projetar uma estratégia apropriada de proteção do ativo de informação;
- Determinar os riscos que possam afetar os ativos de informação;
- Desenvolver as estratégias de tratamento (contingenciamento) de riscos.

A definição da posse de um ativo de informação deve estar associada ao papel ou ao cargo do responsável dentro da organização e não a uma pessoa específica.

3.2.5. Atividade 4 – Identificar os Contêineres dos Recursos

A finalidade desta etapa é listar todos os *recipientes* em que um ativo de informação é armazenado, transportado ou processado e quem são os responsáveis por manter estes *recipientes*. Pode ser executada paralelamente à Atividade 3, porque não há nenhuma dependência entre as duas atividades.

Num processo de avaliação de riscos, a identificação dos contêineres é essencial para identificar os riscos associados à informação. Os ativos de informação são protegidos a partir dos seus respectivos contêineres. É protegendo o contêiner que se inicia a proteção ao ativo de informação. Da mesma forma, o ativo de informação herda os riscos aos quais seus contêineres estão sujeitos. De maneira geral, os contêineres podem ser subdivididos em quatro categorias:

- Sistemas e aplicações;
- Hardwares;
- Pessoas;
- Outros.

Algumas questões básicas podem ser úteis para identificar contêineres:

- Qual sistema de informação ou aplicação usa ou processa determinada informação?
- Em quais plataformas (*software*) os ativos de informação podem ser encontrados?
- Que pessoas têm acesso à informação? Essas pessoas podem ser agrupadas?
- Algum processo automático depende do recurso da informação?
- Que tipos de mídias são utilizados para armazenar a informação?
- A informação é frequentemente impressa, quem pode imprimi-la e onde as cópias impressas são armazenadas?

- Pessoas externas à instituição têm acesso à informação?
- Existem cópias de segurança externas em contratos com terceiros?
- Existem locais de armazenamento físico da informação (papel, mídias magnéticas, etc.)?

3.2.6. Atividade 5 - Definir os Requisitos de Seguranças

Nesta atividade, os requisitos de segurança da informação devem ser definidos por meio de critérios que atendam a disponibilidade, integridade, confidencialidade e autenticidade dessa informação. Se um responsável por um ativo de informação não for capaz de apropriadamente definir os requisitos de segurança desse ativo, não será possível protegê-lo efetivamente.

Podem ser fontes primárias de requisitos de segurança: acordos, contratos, leis, relacionamento com outros ativos de informação, expectativas das partes interessadas e exigências do serviço.

3.2.7. Atividade 6 - Estabelecer o Valor do Ativo de Informação

Antes que os riscos de um ativo de informação possam ser devidamente avaliados, um valor, tangível ou não, deve ser determinado ao ativo.

O responsável pelo ativo de informação e as partes interessadas devem determinar o valor do ativo para a instituição. O valor do ativo deve refletir o quão ele é importante para que a organização alcance seus objetivos. Sob outro prisma, as vezes é mais fácil definir o valor do ativo quando se considera o quão impactante será sua indisponibilidade.

Normalmente o valor do ativo de informação não está nele mesmo, mas no processo de negócio que ele suporta.

Dado o valor, será mais fácil para a administração do Tribunal analisar o custo/benefício para proteger o ativo.

3.3. Fronteiras dos Ativos da Informação

A informação pode ser entendida como a comunicação da inteligência ou do conhecimento do serviço.

Os dados – elementos utilizados como insumos para cálculos, discussões e raciocínios – são componentes essenciais da informação.

A transformação dos dados em informação ocorre da necessidade da organização em mesclar tais dados num certo contexto, o qual agrega valor.

O contínuo ciclo que move os dados através do processo de criar novas informações resulta no desafio de determinar os limites dos recursos de informação.

A determinação de novos requisitos de segurança pode despertar os seguintes questionamentos:

- O novo ativo de informação é substancialmente diferente daqueles os quais lhe deram origem? É realmente "novo"?
- Quem é o responsável pelo novo recurso? É o mesmo dos recursos originários?

- Quais são os requisitos de segurança do novo recurso de informação? A simples combinação dos requisitos de segurança dos ativos originários é suficiente para manter o novo ativo ou é necessário definir um novo requisito?
- Os novos ativos requerem tratamento mais detalhado ou mais simplificado do que os ativos anteriores?

3.4. **Contêineres dos Ativos de Informação**

O contêiner é o local onde "vive" o ativo de informação.

Geralmente o contêiner descreve o tipo da tecnologia - *hardware*, *software*, um sistema de informação - ou até mesmo pessoas, papéis ou mídias magnéticas.

Em outras palavras, o contêiner é qualquer tipo de "recurso" onde a informação está armazenada, é transportada ou processada.

É neste conceito que se percebe que nem todo ativo de informação é digital.

Há três pontos importantes a respeito da segurança e do conceito de contêineres:

- A proteção e a segurança do ativo de informação dependem do nível de segurança implantado no contêiner;
- O grau de proteção e segurança de um ativo depende da eficácia da segurança implantada no contêiner e o quanto tal segurança está alinhada com os requisitos exigidos pelo ativo;
- O ativo de informação herda quaisquer riscos aos quais está sujeito seu contêiner. Desta forma, quando se avalia riscos para um recurso de informação, as vulnerabilidades de seu contêiner devem ser consideradas.

3.5. **Levantamento de Ativos da Informação**

Aqui são apresentados o Formulário de Informações Gerais do Ativo de Informação e o Questionário de Mapeamento de Ativos de Informação.

O Formulário de Informações Gerais do Ativo de Informação visa estruturar as informações coletadas durante as atividades e auxiliar o processo de identificação e classificação de ativos de informação, sendo utilizado em conjunto com o Questionário de Mapeamento de Ativos de Informação.

O Questionário de Mapeamento de Ativos de Informação visa um entendimento comum e inequívoco a respeito do(s) responsável(is), do(s) contêiner(es), dos requisitos de segurança e do valor do ativo de informação e (ii). Além de subsídios para identificação de potenciais ameaças e vulnerabilidades e para a avaliação de riscos como instrumentos de acompanhamento.

3.6. Formulário de Informações Gerais do Ativo de Informação

Informações Gerais do Ativo de Informação		
Data	**Versão**	**Identificação Única**
Responsáveis pelo Preenchimento (nome, cargo/função, área, ramal, e-mail)		
Nome do Ativo		**Impacto no Serviço (alto, médio, baixo)**
Descrição Detalhada		
Responsáveis pelo Ativo de Informação (nome, cargo/função, área, ramal, e-mail)		

Contêineres do Ativo da Informação	
1. **Aplicações e Sistemas**	
Aplicativos de Usuários	
Sistemas Operacionais	
Sistemas Corporativos	
Outros Softwares	
2. **Hardwares**	
Servidores	

Storages	
Estações de Usuários	
Outros Hardwares	
3. **Pessoas**	
Especialistas	
Fornecedores	
Outras Pessoas	
4. **Outros Contêineres**	
Locais Físicos	
Papel	
Mídias Magnéticas	
Outros	

3.7. Questionário de Levantamento de Ativos da Informação

3.7.1. A que área (e.g., seção) pertence o ativo de informação?

_____

3.7.2. Há quanto tempo o ativo de informação está em operação?

a) Menos de 02 anos;

b) Mais de 02 e menos de 05 anos;

c) Mais de 05 e menos de 10 anos;

d) Mais de 10 anos.

3.7.3. O ativo de informação dá suporte a processos associados a:

a) Pleitos eleitorais;

b) Atendimento ao eleitor;

c) Planejamento de ações estratégicas;

d) Processos judiciais eleitorais;

e) Outro. Especificar _____.

3.7.4. Que "áreas de negócio" se relacionam diretamente com o ativo de informação?

a) Pleitos eleitorais;

b) Processos judiciais;

c) Sistemas de informação / rede de comunicação;

d) Administração;

e) Outro. Especificar _____.

3.7.5. Que serviço depende diretamente do ativo de informação?

a) Processos judiciais;

b) Atendimento ao eleitor;

c) Pleitos eleitorais;

d) Outro. Especificar _____.

3.7.6. Qual o nível de classificação do ativo de informação?

a) Fundamentalmente estratégico;

b) Altamente estratégico;

c) Moderadamente estratégico;

d) Levemente estratégico;

e) Pouco estratégico.

3.7.7. Considerando o tempo de existência do ativo de informação, é possível classificá-lo com um alvo:

a) Com ataques em quantidade que justifica mudança imediata nas estratégias de proteção;

b) Com ataques em quantidade significativa;

c) Com ataques em quantidade moderada;

d) Com ataques em quantidade rara;

e) Não há histórico de ataques a este ativo de informação.

3.7.8. Considerando o tempo de existência do ativo de informação, é possível classificá-lo com um alvo:

a) Com perdas em quantidade que justifica mudança imediata nas estratégias de proteção;

b) Com perdas em quantidade significativa;

c) Com perdas em quantidade moderada;

d) Com perdas em quantidade pouco significativa;

e) Não há histórico de perdas neste ativo de informação.

3.7.9. O ativo de informação está localizado em área:

a) Sujeita a desastres naturais em quantidade que justifica mudança imediata nas estratégias de proteção;

b) Sujeita a desastres naturais em quantidade significativa;

c) Sujeita a desastres naturais em quantidade moderada;

d) Sujeita a desastres naturais em quantidade pouco significativa;

e) Sem histórico de desastres naturais.

3.7.10. O Ativo de Informação está Localizado em Área:

a) Sujeita a perturbações/manifestações em quantidade que justifica mudança imediata nas estratégias de proteção;

b) Sujeita a perturbações/manifestações em quantidade significativa;

c) Sujeita a perturbações/manifestações em quantidade moderada;

d) Sujeita a perturbações/manifestações em quantidade pouco significativa;

e) Sem histórico de perturbações/manifestações.

3.7.11. O ativo de informação está em uma plataforma tecnológica:

a) Com arquitetura proprietária;

b) Arquitetura aberta;

c) Arquitetura mista (componentes proprietários e componentes abertos);

d) Não se aplica.

3.7.12. O ativo de informação possui:

a) Dependência de fornecedor exclusivo do mercado externo;

b) Dependência de fornecedor exclusivo do mercado interno;

c) Relativa facilidade de substituição;

d) Não há dependência de fornecedor.

3.7.13. Quanto à governança do ativo de informação:

a) Própria;

b) Compartilhada com múltiplos parceiros nacionais;

c) Compartilhada com parceiros nacionais e internacionais;

d) Depende de um único responsável nacional;

e) Depende de um único responsável internacional.

3.7.14. Como o ativo de informação está estruturado/composto?

a) 100% informatizado;

b) Parcialmente informatizado;

c) Consiste em dados e informações físicas (em papel ou outra forma de armazenamento).

3.7.15. O ativo de informação conta com suporte técnico:

a) Próprio;

b) Terceirizado;

c) Misto;

d) Suporte técnico inexistente ou inadequado.

3.7.16. Qual é o grau de conectividade do ativo de informação com as redes de informação?

a) Conectado diretamente à Internet;

b) Conectado à rede interna da organização;

c) Conectado a uma rede de terceiros;

d) Não está conectado a uma rede;

e) Não se aplica.

3.7.17. O ativo de informação está sujeito a riscos cujo fator gerador é:

a) Humano e intencional;

b) Humano mas não intencional;

c) Eventos naturais;

d) Falhas técnicas.

3.7.18. Qual a expectativa de retorno à normalidade, caso o ativo de informação sofra algum sinistro?

a) Até 02 horas;

b) Até 10 horas;

c) Até 24 horas;

d) Até 72 horas;

e) Mais e 72 horas.

3.7.19. Se houve incidentes que comprometeram o ativo de informação nos últimos três anos, qual foi o tempo médio de retorno à normalidade com os procedimentos de contingência?

a) Até 02 horas;

b) Até 10 horas;

c) Até 24 horas;

d) Até 72 horas;

e) Mais e 72 horas;

f) Não foi possível restaurar.

3.7.20. Caso haja histórico de incidentes, que tipo de incidente já comprometeu o ativo de informação?

a) Ataque bem sucedido;

b) Desastre natural;

c) Incêndio;

d) Roubo/furto;

e) Outro. Especificar _____.

3.7.21. Caso haja histórico de incidentes, o que originou a maioria dos incidentes?

a) Ataques intencionais provenientes do ambiente externo;

b) Ataques intencionais provenientes do ambiente interno da organização;

c) Ataques não intencionais provenientes do ambiente externo;

d) Ataques não intencionais provenientes do ambiente interno da organização;

e) Fenômenos naturais;

f) Não foi possível identificar.

3.7.22. Existe algum entrave a ser superado para a gestão o ativo de informação?

a) A dimensão e/ou a complexidade da infra-estrutura tecnológica envolvida;

b) A interdependência dos processos que envolvem este ativo;

c) Existência de múltiplas normas e padrões técnicos;

d) Conflito entre segurança e privacidade;

e) Questões legais;

f) Questões geográfico-climáticas;

g) Capacitação de RH;

h) Ampliação da segurança das redes;

i) Falta de divisão clara de responsabilidades entre vários agentes intervenientes;

j) Questões internas da Organização;

k) Outro. Especificar _____.

3.7.23. Há algum entrave para implantar um plano de contingência e recuperação do ativo de informação?

a) Orçamentário;

b) De ordem técnica;

c) Falta de capacitação de pessoal;

d) De ordem legal;

e) Outro. Especificar _____.

3.7.24. Que ações já ocorrem para a proteção do ativo de informação?

a) Identificação de vulnerabilidades;

b) Análise de riscos;

c) Plano de contingência;

d) Capacitação de pessoal para contingência de incidentes/desastres;

e) Suporte técnico terceirizado especializado.

3.7.25. Em situação de incidente/desastre com o ativo de informação, os danos comprometem que áreas?

a) Pleitos eleitorais;

b) Processos judiciais;

c) Sistemas de informação / rede de comunicação;

d) Administração;

e) Outro. Especificar _____.

3.7.26. Em situação de incidente/desastre com o ativo de informação, quais seriam as extensões do dano?

a) Prejuízo interno no Tribunal;

b) Prejuízo na esfera da Justiça Eleitoral;

c) Prejuízo na esfera da administração pública;

d) Prejuízo à população;

e) Outro. Especificar _____.

3.7.27. Um ataque bem sucedido ao ativo de informação poderia se propagar em que escala?

a) Outras áreas no Tribunal;

b) Outros órgãos da Justiça Eleitoral;

c) Outros órgãos da administração pública;

d) Prejuízo à população;

e) Outro. Especificar _____.

3.7.28. Qual o nível de impacto em caso de comprometimento do ativo de informação?

a) Apropriação indevida de funções do ativo de informação;

b) Problemas no processo relacionado ao ativo de informação;

c) Problemas no serviço da área responsável pelo ativo de informação;

d) Problemas no serviço de outras áreas;

e) Problemas nos serviços ao público.

3.7.29. Quem realiza auditoria/fiscalização/verificação no ativo de informação?

a) A área responsável pelo ativo de informação;

b) A administração do Tribunal;

c) Órgão externo, regulador;

d) Auditoria terceirizada, contratada;

e) Não há auditoria/fiscalização.

3.7.30. O ativo de informação está subordinado a que nível?

a) Decisório (administração);

b) Estratégico (planejamento);

c) Tático (assessorias, coordenações);

d) Operacional (áreas meio e fim);

e) Colegiados/comissões.

3.7.31. Em caso de incidente/perda, qual é a capacidade de recuperação do ativo de informação?

a) Recuperação total;

b) Recuperação parcial com perdas insignificantes;

c) Recuperação parcial com perdas significativas;

d) Irrecuperável.

3.7.32. Os impactos no ativo de informação são limitados geograficamente à dimensão:

a) Local;

b) Municipal;

c) Estadual;

d) Nacional.

3.8 REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 27001:2006**: Tecnologia da Informação: Técnicas de Segurança da Informação: Sistemas de Gestão de Segurança da Informação: Requisitos. Rio de Janeiro, 2006.

ABNT. **ABNT NBR ISO/IEC 27002:2005**: Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ABNT. **ABNT NBR ISO/IEC 27005:2008**: Tecnologia da Informação: Técnicas de Segurança: Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008a.

ABNT. **ABNT NBR 15999-1:2007**: Gestão de Continuidade de Negócios - Parte 1: Código de prática. Rio de Janeiro, 2007.

ABNT. **ABNT NBR 15999-2:2008**: Gestão de Continuidade de Negócios - Parte 2: Requisitos. Rio de Janeiro, 2008b.

ABNT. **ABNT NBR ISO 31000:2009**: Gestão de riscos - Princípios e diretrizes. Rio de Janeiro, 2009a.

ABNT. **ABNT ISO GUIA 73:2009**: Gestão de riscos - Vocabulário. Rio de Janeiro, 2009b.

STEVENS, J. F. Information Asset Profiling: CMU – Carnegie Mellon University, June 2005. 61 p. (CMU/SEI-2005-TN-021). Disponível em: <www.cert.org/archive/pdf/05tn021.pdf>. Acesso em: Maio, 2012.