

Planejamento Estratégico de TI

DTIN / ON

Observatório Nacional





ÍNDICE

1. INTRODUÇÃO - CONCEITOS BÁSICOS E DIRETRIZES	6
1.1. GOVERNANÇA DE TI.....	6
1.2. COBIT – “CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY”.....	7
1.3. ISACA – “INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION”	8
1.4. GERENCIAMENTO DE SERVIÇOS DE TI – ITIL V3.....	8
1.5. OGC - OFFICE OF GOVERNMENT COMMERCE	9
1.6. NORMA ABNT NBR ISO/IEC 20000-1	9
1.7. NORMA ABNT NBR ISO/IEC 27001.....	10
1.8. AVALIAÇÃO DE MATURIDADE DE PROCESSOS DE TI.....	10
1.9. SECRETÁRIA DE LOGISTICA E TECNOLOGIA DA INFORMAÇÃO - SLTI.....	10
1.10. DIRECIONADORES ESTRATÉGICOS.....	11
1.11. TRIBUNAL DE CONTAS DA UNIÃO	13
2. CONTEXTUALIZAÇÃO	16
3. OBJETIVO DO TRABALHO	17
3.1. LEVANTAMENTO E ANÁLISE DOS PROCESSOS DE TI.....	17
3.2. DIAGNÓSTICO DOS PROCESSOS DE TI COM BASE MODELO DE MATURIDADE PARA CONTROLES INTERNOS	18
3.3. ELABORAÇÃO DE PLANO DE AÇÃO DE CURTO, MÉDIO E LONGO PRAZO	23
4. DIAGNÓSTICO DA SITUAÇÃO ATUAL DE TI DA DTIN/ON E PLANO DE AÇÃO DE CURTO PRAZO	24
4.1. DIAGNÓSTICO GOVERNANÇA DE TI (PROCESSOS ESTRATÉGICOS)	29



4.1.1. DIAGNÓSTICO MISSÃO E VISÃO DA TI	30
4.1.2. DIAGNÓSTICO PLANEJAMENTO ESTRATÉGICO DE TI ALINHADO AOS OBJETIVOS DE NEGÓCIO	30
4.1.3. DIAGNÓSTICO ESTRATÉGIA E PADRÕES TECNOLÓGICOS	30
4.1.4. DIAGNÓSTICO ESTRUTURA ORGANIZACIONAL DE TI	30
4.1.5. ARQUITETURA DA INFORMAÇÃO EMPRESARIAL	31
4.1.6. VISÃO DA ESTRATÉGIA DOS SERVIÇOS	31
4.1.7. MELHORIA DOS SERVIÇOS	31
4.2. DIAGNÓSTICO GESTÃO DE PROJETOS E PROCESSOS DE TI (PROCESSOS TÁTICOS E OPERACIONAIS)	32
4.2.1. GESTÃO DE PROJETOS DE TI	32
4.2.2. GESTÃO DE PROCESSOS DE TI	32
4.2.3. CENTRAL DE SERVIÇOS	33
4.2.4. GERENCIAMENTO DAS APLICAÇÕES	33
4.2.5. GERENCIAMENTO DE OPERAÇÕES	34
4.2.6. GERENCIAMENTO TÉCNICO	34
4.3. DIAGNÓSTICO SERVIÇOS, SISTEMAS E APlicativos	34
4.3.1. SISTEMAS DE USO CORPORATIVO	34
4.3.2. DIVISÃO ADMINISTRATIVA - SERVIÇO DE RECURSOS HUMANOS	35
4.3.3. DIVISÃO ADMINISTRATIVA - SERVIÇO FINANCEIRO	36
4.3.4. DIVISÃO ADMINISTRATIVA - SERVIÇO DE MATERIAL E PATRIMÔNIO	36
4.3.5. DIVISÃO ADMINISTRATIVA - SERVIÇO DE APOIO LOGÍSTICO	37
4.3.6. DIVISÃO DE INFORMAÇÕES E DOCUMENTAÇÃO	37
4.3.7. COORDENAÇÃO DE ASTRONOMIA E ASTROFÍSICA	37
4.3.8. GRUPO DE PESQUISA EM ASTRONOMIA - GPA	38



4.3.9. COORDENAÇÃO DE GEOFISICA	38
4.3.10. DIVISÃO DE PÓS-GRADUAÇÃO	39
4.3.11. DIVISÃO DE SERVIÇO DA HORA.....	39
4.3.12. DIVISÃO DE ATIVIDADES EDUCACIONAIS	40
4.4.DIAGNÓSTICO DE RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	40
5. RECOMENDAÇÕES	42
5.1.GOVERNANÇA DE TI.....	42
5.2.GESTÃO DE PROJETOS E PROCESSOS DE TI.....	42
5.3.SERVIÇOS, SISTEMAS E APLICATIVOS.....	43
5.4.RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	43
6. PRIORIDADE DOS PROJETOS.....	45
6.1 1ª ONDA - AÇÕES DE CURTO PRAZO.....	46
6.1.1. GOVERNANÇA DE TI.....	46
6.1.2. GESTÃO DE PROJETOS E PROCESSOS.....	49
6.1.3. SERVIÇOS, SISTEMAS E APLICATIVOS.....	50
6.1.4. RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	52
6.2 2ª ONDA - AÇÕES DE MÉDIO PRAZO.....	54
6.2.1. GOVERNANÇA DE TI.....	54
6.2.2. GESTÃO DE PROJETOS E PROCESSOS.....	55
6.2.3. SERVIÇOS, SISTEMAS E APLICAÇÕES	56
6.2.4. RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	57
6.3 3ª ONDA – 24 MESES	59
6.3.1. GOVERNANÇA DE TI.....	59



6.3.2. GESTÃO DE PROJETOS E PROCESSOS.....	60
6.3.3. SERVIÇOS, SISTEMAS E APLICAÇÕES	61
6.3.4. RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	62



1. INTRODUÇÃO - CONCEITOS BÁSICOS E DIRETRIZES

1.1. GOVERNANÇA DE TI

Cada vez mais os serviços e a gestão nas Organizações apoiam-se no uso da Tecnologia da Informação (TI) e de sistemas de informação. Torna-se necessário, portanto, um efetivo alinhamento e integração entre o direcionamento da TI e os objetivos estratégicos da instituição.

A Governança de TI é responsabilidade de dirigentes e conselhos de administração e compreende a liderança, estruturas organizacionais e processos que asseguram que a Tecnologia da Informação sustenta e amplia as estratégias e objetivos da instituição.

É responsabilidade da Governança assegurar que:

- a. TI preste os serviços alinhados com as estratégias institucionais.
- b. TI e as novas tecnologias sejam utilizadas para introduzir inovações em processos, produtos/serviços e melhorar o desempenho organizacional.
- c. Os serviços e as funcionalidades sejam oferecidos com a maior eficácia de custos e de maneira mais eficiente possível.
- d. Todos os riscos de TI sejam conhecidos e que seus recursos (informações, sistemas, equipamentos, etc.) estejam seguros.



1.2. COBIT – “CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY”

O COBIT, atualmente na versão 4.1, é um conjunto de melhores práticas em um “framework” de domínios e processos, resultado do consenso de “experts” internacionais. É, reconhecidamente, o único “framework” que abrange todas as áreas de TI. Ele é muito útil na formalização dos processos e controles internos, como ferramenta de auxílio na otimização dos investimentos em TI, alinhamento estratégico, gestão de riscos, em assegurar entrega de serviços e proporcionar uma medida de desempenho, falhas e vulnerabilidades.

O COBIT suporta a Governança de TI, ao proporcionar uma estrutura que assegura que:

- TI está alinhada com o negócio ou com os serviços da instituição ou de seus clientes;
- TI habilita o negócio ou o serviço e maximiza benefícios;
- Os recursos de TI são usados de forma responsável;
- Os riscos de TI são gerenciados de forma apropriada.

O COBIT pode ser utilizado identificando responsabilidades e requisitos de controle como critérios de avaliação, subsidiando pareceres e recomendando ações gerenciais de fortalecimento de controles internos e de aperfeiçoamento dos processos de TI.



Este modelo é mantido pelo Instituto de Governança de TI (ITGI) e pela Associação dos Controladores e Auditores de Sistemas de Informação (ISACA), que são as duas organizações reconhecidas mundialmente como promotoras da governança de TI.

1.3. ISACA – “INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION”

A ISACA é uma associação internacional, formada exclusivamente por profissionais que atuam nas áreas de Auditoria de Sistemas, Segurança da Informação e, principalmente, de Governança de TI. Iniciou suas atividades em 1967, com um pequeno grupo de Auditores que atuavam em Empresas nas quais os sistemas informatizados começavam cada vez mais desempenhar operações críticas. Os associados da ISACA vivem e atuam em mais de 140 Países e compreendem uma grande variedade de posições relativas à Tecnologia da Informação (entre outras: Auditores de SI, Consultores, Profissionais de Segurança de TI, CIO's e Auditores Internos). É importante notar que a maioria dos Associados desempenham funções na alta e média gerência dessas atividades, exercidas em empresas e organizações de todos os segmentos econômicos – indústria, comércio, finanças, governo, etc.

1.4. GERENCIAMENTO DE SERVIÇOS DE TI – ITIL V3

O Diagnóstico do Gerenciamento de Serviços de TI foi elaborado com a finalidade de examinar a maturidade e a qualidade dos processos de Gerenciamento de Serviços de Tecnologia da Informação do Observatório Nacional - ON, com base nas melhores práticas recomendadas em ITIL® (Information Technology Infrastructure Library) do OGC (Office of Government Commerce) e, também, experiência da PATH ITTS.



1.5. OGC - OFFICE OF GOVERNMENT COMMERCE

É um escritório independente do Tesouro britânico, criado para ajudar o governo demonstrar o melhor investimento de seus gastos.

1.6. NORMA ABNT NBR ISO/IEC 20000-1

Esta parte da ISO/IEC 20000 define os requisitos para que um provedor de serviço possa gerenciar o fornecimento de serviços com qualidade aceitável para seus clientes.

Pode ser utilizado:

- Por empresas que estão buscando oferecer seus serviços;
- Por empresas que requeiram uma abordagem consistente, por parte de todos os provedores de serviços, numa cadeia de suprimentos;
- Por fornecedores de serviço para compararem sua Gerência de Serviços em TI;
- Como base para uma avaliação independente;
- Por uma instituição que necessite demonstrar habilidade para fornecer serviços que atendam as necessidades do cliente;
- Por uma instituição que vise melhorar seus serviços através da aplicação efetiva de processos para monitorar e melhorar a qualidade do serviço.



1.7. NORMA ABNT NBR ISO/IEC 27001

Esta Norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A especificação e a implementação do SGSI de uma instituição são influenciadas pelas necessidades e objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da instituição. Esta norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas.

1.8. AVALIAÇÃO DE MATURIDADE DE PROCESSOS DE TI

Consiste no exame dos processos, suas atividades e dos sistemas de suporte que trafegam, processam ou armazenam informações, com a finalidade de verificar se sua execução, operação e funcionamento estão em conformidade com determinados objetivos e normas que estabelecem condições mínimas de desempenho, qualidade, controle, gerenciamento de risco e segurança da informação.

1.9. SECRETÁRIA DE LOGISTICA E TECNOLOGIA DA INFORMAÇÃO - SLTI

O SECRETÁRIO DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO DO MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO E PRESIDENTE DA COMISSÃO DE COORDENAÇÃO DO SISP - Sistema de Administração de Recursos de Informação e Informática, no uso das atribuições,..resolve:



Art. 1º Aprovar a Estratégia Geral de Tecnologia da Informação (EGTI) versão 2010 para a Administração Pública Federal direta, autárquica e fundacional do Poder Executivo Federal, na forma do Anexo a esta Resolução.

O planejamento de ações de TI deve atender às diretrizes do Comitê Executivo de Governo Eletrônico - CEGE, relacionadas a seguir:

- A) a promoção da cidadania como prioridade;
- B) a inclusão digital é indissociável do governo eletrônico;
- C) o software livre é um recurso estratégico para a implementação do governo eletrônico;
- D) a gestão do conhecimento como instrumento estratégico de articulação e gestão das políticas públicas;
- E) o governo eletrônico deve racionalizar os recursos;
- F) o governo eletrônico deve contar com um arcabouço integrado de políticas, sistemas, padrões e normas;
- G) a integração das ações de governo eletrônico com outras esferas e poderes.

1.10. DIRECIONADORES ESTRATÉGICOS

Fortalecimento

1. TI passa a ser estratégica ao atender as áreas fins e o cidadão diretamente.
2. Empoderar (fortalecer) gestores de TI.
3. Capacitar, qualificar e reter pessoal alinhado com direcionador 1.
4. Fortalecer o poder de coordenação e mobilização de TI.
5. Investir em ações de fortalecimento da credibilidade da TI

6. Projetar ações para favorecer a participação de TI nos planejamentos estratégicos.

Alinhamento

1. Alinhar área de TI às políticas públicas e diretrizes prioritárias.
2. Tomar ações para favorecer a transparência.
3. Desenvolver competência/carreira entre profissionais de TI.
4. Desenvolver competência para aproximação da linguagem utilizada por TI com a utilizada pelas áreas de negócio e o cidadão.
5. Estruturar a governança de TI favorecendo o alinhamento das ações de TI com as áreas de negócio.
6. Firmar parceiras com as áreas de comunicação dos órgãos do Governo Federal.
7. Investir na disponibilidade e integridade das informações do Governo.

Integração

1. Compartilhar soluções meio (ex.: administrativas) em TI do Governo Federal.
2. Integrar e produzir sinergia nas coordenadorias e área de TI numa base contínua
3. Integrar processos e sistemas.

Desenvolvimento de Capacidades

1. Investir em aumento da produtividade e otimização dos recursos.

2. Focalizar-se na gestão do conhecimento.
3. Encaminhar o dilema centralização x descentralização dentro das tendências e melhores práticas.
4. Investir na capacitação dos altos dirigentes e usuários em TI.
5. Investir na adoção de melhores práticas.

1.11. TRIBUNAL DE CONTAS DA UNIÃO

Planejamento Estratégico

A recomendação registrada no item 9.1.1 do Acórdão nº 1.603/2008-TCU-Plenário aos órgãos governantes superiores foi a seguinte:

"9.1.1. promovam ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da instituição;"

Estrutura de Pessoal de TI

A recomendação registrada no item 9.1.2 do Acórdão nº 1.603/2008-TCU-Plenário aos órgãos governantes superiores foi a seguinte:

"9.1.2. atentem para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor, garantindo, outrossim, sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição".

Segurança da Informação

A recomendação registrada no item 9.1.3 do Acórdão nº 1.603/2008-TCU-Plenário aos órgãos governantes superiores foi a seguinte:

“9.1.3 orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;”

Desenvolvimento de Software

A recomendação contida no Acórdão nº 1.603/2008-TCU-Plenário aos órgãos governantes superiores foi a seguinte:

“item 9.1.4. estimulem a adoção de metodologia de desenvolvimento de sistemas, procurando assegurar, nesse sentido, níveis razoáveis de padronização e bom grau de confiabilidade e segurança;”

Gestão de Níveis de Serviço

A recomendação contida no Acórdão nº 1.603/2008-TCU- Plenário aos órgãos governantes superiores foi a seguinte:

“item 9.1.5: promovam ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da instituição;”

Processo de Contratação e Gestão de Contratos de TI

A recomendação contida no Acórdão nº 1.603/2008-TCU-Plenário aos órgãos governantes superiores foi a seguinte:

"item 9.1.6. evidem esforços visando à implementação de processo de trabalho formalizado de contratação de bens e serviços de TI, bem como de gestão de contratos de TI, buscando a uniformização de procedimentos nos moldes recomendados no item 9.4 do Acórdão 786/2006-TCU-Plenário;"

A recomendação contida no Acórdão 786/2006-TCU-Plenário foi a seguinte:

9.4.3. a mensuração, sempre que possível, da prestação de serviços por resultados segundo especificações previamente estabelecidas, evitando-se a mera locação de mão-de-obra e o pagamento por hora-trabalhada ou por posto de serviço, utilizando-se de metodologia expressamente definida no edital que contemple, entre outros, os seguintes pontos básicos:

9.4.3.1. a fixação dos procedimentos e dos critérios de mensuração dos serviços prestados, abrangendo métricas, indicadores, valores aceitáveis, etc.; 9.4.3.2. a quantificação ou a estimativa prévia do volume de serviços demandados, para fins de comparação e controle; 9.4.3.3. a definição de metodologia de avaliação da adequação às especificações e da qualidade dos serviços com vistas à aceitação e pagamento; 9.4.3.4. a utilização de um instrumento de controle, geralmente consolidado no documento denominado "ordem de serviço" ou "solicitação de serviço"; 9.4.3.5. a definição dos procedimentos de acompanhamento e fiscalização a serem realizados concomitantemente à execução para evitar distorções na aplicação dos critérios; 9.4.4. a utilização, como instrumento de controle das etapas de solicitação, acompanhamento, avaliação, atestação e pagamento de serviços, da "ordem de serviço" ou "solicitação de serviço", que deve conter, no mínimo: 9.4.4.1. a definição e a especificação dos serviços a serem realizados; 9.4.4.2. o volume de serviços solicitados e realizados segundo as métricas definidas; 9.4.4.3. os resultados ou produtos solicitados e realizados; 9.4.4.4. o cronograma de realização dos serviços, incluídas todas as tarefas significativas e seus respectivos prazos; a avaliação da qualidade dos serviços realizados e as justificativas do avaliador; 9.4.4.6. a identificação dos responsáveis pela solicitação, pela avaliação da qualidade e pela atestação dos serviços realizados, os quais não podem ter nenhum vínculo com a empresa contratada;

A recomendação contida no Acórdão n.º 947/2010-Plenário foi a seguinte:

b) "incluir no termo de referência, em atendimento ao princípio da eficiência e com base nas orientações disponíveis no item 9.4 do Acórdão nº 786/2006-TCU-Plenário, no item 9.1.1 do Acórdão nº 1.215/2009-TCU-Plenário, na Instrução Normativa SLTI/MP nº 4/2008 e na norma ABNT ISO/IEC NBR 20000:2008, claro detalhamento do nível de



serviço necessário à execução do objeto, com a definição de cada resultado esperado, inclusive quanto a prazo e qualidade aceitáveis, dos mecanismos de aferição da qualidade e do desempenho e dos mecanismos de segregação de funções, que assegure a não ocorrência de conflito de interesse na medição e remuneração de serviços;”.

Processo Orçamentário de TI

A recomendação contida no Acórdão 1.603/2008-TCU-Plenário aos órgãos governantes superiores foi a seguinte:
“item 9.1.7. adotem providências com vistas a garantir que as **propostas orçamentárias para a área de TI** sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos do negócio;”

Auditoria de TI

A recomendação contida no Acórdão nº 1.603/2008-TCU-Plenário aos órgãos governantes superiores foi a seguinte:
“item 9.1.8. introduzam práticas voltadas à realização de auditorias de TI, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados;”

2. CONTEXTUALIZAÇÃO

Dessa forma, o diagnóstico do ambiente constitui-se no primeiro passo para montar a infraestrutura necessária à realização periódica de avaliação dos referidos processos quanto ao seu nível de maturidade que corresponde à capacidade de atender às necessidades e expectativas do Observatório Nacional - ON.



3. OBJETIVO DO TRABALHO

As atividades foram realizadas com base na documentação disponibilizada pela Gerência de Tecnologia da Informação – DTIN – do Observatório Nacional dentro do seu ambiente, tendo a estrutura do COBIT 4.1, MPSBR, ITIL V3, ABNT NBR ISO/IEC 20000-1 e ABNT NBR ISO/IEC 27001 como ferramenta e a análise do nível de maturidade de processos como foco principal.

3.1. LEVANTAMENTO E ANÁLISE DOS PROCESSOS DE TI.

O levantamento das informações sobre os processos foi obtido através da disponibilização de documentos de processos, procedimentos, formulários e relatórios de indicadores.

Além das fontes citadas acima, foram colhidas informações por meio de entrevistas com os gestores operacionais, os quais possuem as funções de proprietários e gestores de processos. Estas informações foram registradas em relatórios de entrevistas.

Esta etapa da metodologia tem por objetivo colher documentos e relatos sobre o desenvolvimento operacional dos processos, práticas internas, características da cultura organizacional e dificuldades, tanto operacionais, quanto na implementação de práticas.

Durante a realização desta atividade, a equipe de consultores e os representantes da DTIN identificaram o conjunto de informações relevantes de TI, no âmbito do Observatório Nacional - ON, com foco nos procedimentos de avaliação da maturidade e processos, sendo estabelecido o perfil adequado desses procedimentos.

Os critérios e procedimentos adotados estão baseados no COBIT 4.1, MPSBR, ITIL V3, ABNT NBR ISO/IEC 20000-1 e ABNT NBR ISO/IEC 27001.



Visando obter uma visão geral das atividades do Observatório Nacional - ON, foram realizadas:

- Consulta e análise da documentação existente (Instruções, Regulamentos, Regimento Interno, Política do Observatório Nacional - ON para a TI, Normas),
- Entrevistas com dirigentes, gestores de áreas de interesse e gestores de TI do Observatório Nacional - ON.

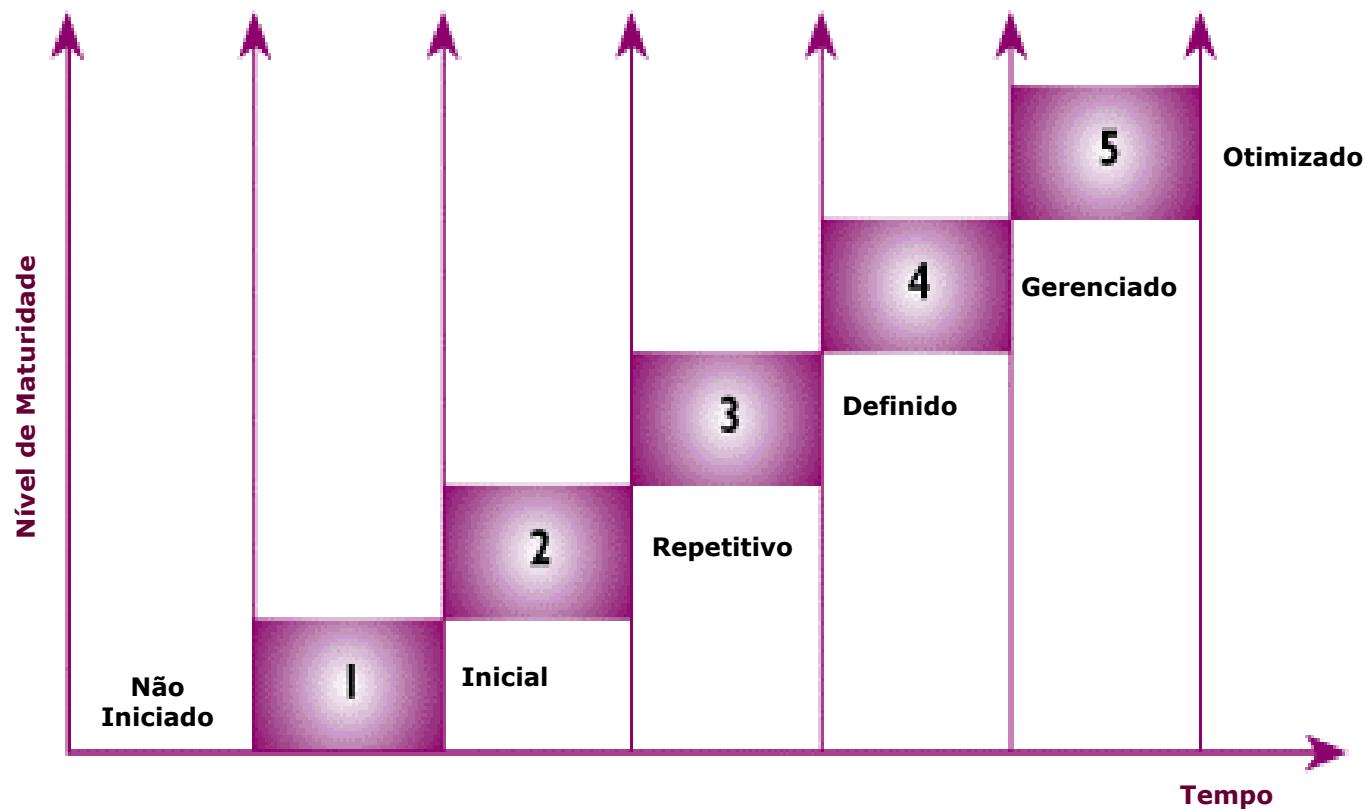
3.2. DIAGNÓSTICO DOS PROCESSOS DE TI COM BASE MODELO DE MATURIDADE PARA CONTROLES INTERNOS

Nesta etapa foram destacados os principais pontos de diferença entre os procedimentos de avaliação dos níveis de maturidade de processos praticados pela Gerência de Tecnologia da Informação – do Observatório Nacional - ON e os modelos específicos e geral de maturidade do COBIT 4.1, MPSBR, ITIL V3, ABNT NBR ISO/IEC 20000-1 e ABNT NBR ISO/IEC 27001.

O modelo adotado possui em sua estrutura duas abordagens para atribuição da maturidade, sendo uma genérica e a outra detalhada por processo com características por nível de maturidade. Abaixo é apresentada a abordagem genérica do modelo de maturidade:

A abordagem de atribuição da maturidade detalhada por processo menciona características para cada processo por nível de maturidade. Esta foi adotada como base de análise, permitindo uma comparação detalhada das características dos processos em cada nível de maturidade.

Cabe ressaltar que nem todas as organizações de TI necessitam ter o mais alto nível. É necessário considerar o papel da TI na instituição e o seu impacto nos objetivos da corporação, sua missão. As principais características de cada nível de maturidade são:





Nível de Maturidade	Estágio do Ambiente de Controle Interno	Estabelecimento de Controles Internos
0 Inexistente	Não existe o reconhecimento da necessidade de controles internos. Controles não são parte da cultura ou missão da empresa. Existe um alto risco de deficiências de controles e de incidentes.	Não existe a intenção de avaliar a necessidade de controles internos. Incidentes são tratados quando aparecem.
1 Inicial / <i>Ad hoc</i>	Existe algum reconhecimento da necessidade de controles internos. O enfoque com relação a riscos e controles é <i>ad hoc</i> e desorganizado, sem comunicação ou monitoramento. Deficiências não são identificadas. Funcionários não estão conscientes de suas responsabilidades.	Não existe a consciência da necessidade da avaliação do que é preciso em termos de controles de TI. Quando é realizado, ocorre somente em base <i>ad hoc</i> , num nível superficial e como reação a incidentes significativos. As avaliações tratam somente dos incidentes ocorridos.
2 Repetível, porém Intuitivo	Controles estão em funcionamento mas não são documentados. A sua operação é dependente do conhecimento e da motivação da pessoas. Efetividade não é adequadamente avaliada. Existem muitas fragilidades de controles e elas não são adequadamente tratadas; o impacto pode ser severo. Ações gerenciais para resolver problemas de controles não são priorizadas ou consistentes. Os funcionários podem não estar conscientes de suas responsabilidades.	Avaliações da necessidade de controles ocorrem quando necessário para processos selecionados de TI visando determinar o nível de maturidade atual, o nível que deveria ser atingido e as lacunas existentes. Uma reunião com enfoque informal, envolvendo gerentes de TI e a equipe envolvida no processo é utilizado para definir um enfoque adequado de controles para o processo e para motivar um plano de ação aceito por todos.



3 Processo Definido	<p>Controles estão em funcionamento e são adequadamente documentados. A efetividade operacional é avaliada periodicamente, e existe um número médio de problemas. No entanto, o processo de avaliação não é documentado. Embora a gerência trate a maioria dos problemas de controle de maneira previsível, algumas fragilidades de controle persistem e os impactos podem ainda ser severos. Os funcionários estão conscientes de suas responsabilidades relacionadas a controles. Os processos críticos de TI são identificados com base em direcionadores de valor e riscos. Uma análise detalhada é realizada para identificar os requisitos de controles e das causas das lacunas, bem como para desenvolver oportunidades de aprimoramento. Além das reuniões facilitadas, ferramentas e entrevistas são executadas para suportar as análises e assegurar que os proprietários de processos de TI dominem e direcionem o processo de avaliação e o aprimoramento.</p>	<p>Os processos críticos de TI são identificados com base em direcionadores de valor e riscos. Uma análise detalhada é realizada para identificar os requerimentos de controles e das causas dos gaps, bem como para desenvolver oportunidades de aprimoramento. Em adição a reuniões facilitadas, ferramentas e entrevistas são executadas para suportar as análises e assegurar que os proprietários de processos de TI dominam e direcionam o processo de avaliação e o aprimoramento.</p>
----------------------------	---	---



4 Gerenciado e Mensurável	<p>Existe um efetivo ambiente de controles internos e gerenciamento de riscos. Uma avaliação formal e documentada dos controles ocorre frequentemente. Muitos controles são automatizados e regularmente revisados. A gerência provavelmente detecta a maioria dos problemas de controle, mas nem todos os problemas são rotineiramente identificados. Existe um contínuo acompanhamento para solucionar as fragilidades de controles. O uso limitado e tático da tecnologia é aplicado para automatizar os controles.</p>	<p>A criticidade de processos de TI é regularmente definida com total suporte e concordância de proprietários de processos de negócios. A avaliação de requisitos de controles é baseado na política e na maturidade desses processos, seguindo uma análise mensurada envolvendo as partes interessadas chaves. A responsabilidade por essas avaliações é clara e incentivada. Estratégias de aprimoramento são suportadas por propostas de negócios. A performance para atingir os resultados desejados é consistentemente monitorada. Revisões de controle externas são organizadas ocasionalmente.</p>
5 Otimizado	<p>Um programa corporativo de risco e controles proporciona uma contínua e efetiva resolução de questões relacionadas a controles e riscos. O gerenciamento de controles internos e riscos é integrado com as práticas corporativas, suportado por um monitoramento automatizado em tempo real, com uma total responsabilização pelo monitoramento dos controles, gerenciamento de riscos e procedimentos para conformidade. A avaliação dos controles é contínua, baseada na auto-avaliação e análises de lacuna e de causa-raiz. Os funcionários estão proativamente envolvidos no aprimoramento de controles.</p>	<p>Mudanças de negócios consideram a criticidade dos processos de TI e cobrem qualquer necessidade para reavaliar a capacidade de controle do processo. Os proprietários de processos de TI realizam autoavaliações frequentes para verificar se os controles estão no nível correto de maturidade a fim de atingir as necessidades de negócios e consideram os atributos de maturidade para encontrar maneiras de tornar os controles mais eficientes e efetivos. A organização faz comparações com boas práticas externas e procura consultoria externa sobre a efetividade dos controles internos. No caso de processos críticos, são realizadas revisões independentes para prover garantia de que os controles estão no nível desejado de maturidade e funcionam como planejado.</p>



3.3. ELABORAÇÃO DE PLANO DE AÇÃO DE CURTO, MÉDIO E LONGO PRAZO

IMPLEMENTAÇÃO EM 3 ONDAS

Considerando o volume e a complexidade dos problemas identificados, as ações propostas foram ordenadas em 3 ondas:

1ª. Onda – duração 8 meses - **ações emergenciais e as de curto prazo** (de Maio/2011 a Dezembro/2011) visando criar condições básicas para o início da implementação da Governança.

2ª. Onda – duração 24 meses - ações que deverão ser deflagradas de Janeiro/2012 a Dezembro/2013, visando reforçar as condições para maior eficiência / eficácia de TI.

3ª. Onda – duração 12 meses - ações que deverão ser deflagradas de Janeiro/2014 a Dezembro/2015, visando melhorar nível de serviços aos clientes internos e externos e da segurança.

Nesta etapa foram destacadas as principais **ações de curto prazo** visando à correção de problemas e ajustes necessários para o fortalecimento da Divisão de Tecnologia da Informação – DTIN do Observatório Nacional - ON.



4. DIAGNÓSTICO DA SITUAÇÃO ATUAL DE TI DA DTIN/ON E PLANO DE AÇÃO DE CURTO PRAZO

O presente documento contempla o Diagnóstico resumido com os principais pontos que subsidiaram o planejamento das ações de curto prazo visando criar condições mínimas para o início da implementação do PDTI do ON e as ações de médio e longo prazo para que a DTIN alcance os objetivos da instituição para a área de tecnologia da informação.

Abaixo as principais forças, fraquezas, ameaças e oportunidades identificadas:

PONTOS FORTES

- A equipe gerencial da DTIN busca dar atendimento as demandas dos usuários dentro do cenário atual;
- Existe conscientização da importância da definição de um plano de arquitetura da informação;
- A equipe gerencial da DTIN reconhece a importância de um plano de infraestrutura de tecnologia;
- A equipe gerencial da DTIN tem perícia e habilidades necessárias para desenvolver o orçamento de TI e recomendar investimentos de TI apropriados;
- A equipe gerencial da DTIN reconhece a importância das necessidades e requisitos de um ambiente efetivo de controle da informação;
- A equipe gerencial da DTIN reconhece a importância de gerenciamento de recursos humanos de TI;
- Existem iniciativas para definir requisitos e identificar soluções de tecnologia;
- A equipe gerencial da DTIN reconhece a necessidade de um processo para definir níveis de serviço;
- A equipe gerencial da DTIN reconhece a necessidade de gerenciar desempenho e capacidade de TI;
- A equipe gerencial da DTIN tem a percepção dos riscos, vulnerabilidades e ameaças às operações de TI ou ao impacto da perda de serviços de TI ao negócio;
- A equipe gerencial da DTIN reconhece a necessidade de um processo de gerenciamento de dados preciso;



- A gerência da DTIN reconhece a necessidade de coletar e avaliar informações sobre os processos de monitoração;
- Existe conscientização da equipe gerencial da DTIN dos requisitos de conformidade, regulatórios, contratuais e legais que impactam a instituição.

□ PONTOS FRACOS

- Falta alinhamento entre os objetivos e metas do ON com a de TI;
- Falta de Modelo de Governança e Gestão de TI;
- O alinhamento aos requerimentos do negócio, aplicações e tecnologia ocupa um espaço reativo em vez de ser uma estratégia de toda instituição;
- O Suporte a Servidores e Rede (nível 2 de atendimento) existe, porem sem padrões, sem documentação e sem domínio da configuração atual;
- O Suporte e atendimento de nível 1 iniciado, porém sem garantia de registro de todos os chamados;
- O Suporte ao desenvolvimento de sistemas existe, porem sem garantia de continuidade para o negócio e fora da gestão da DTIN;
- Modelo de Governança e de Gestão de TI com ações focadas nas necessidades dos departamentos sem visão corporativa;
- Iniciativas de prestação de serviços de TI em nível das áreas, sem existência de Políticas, Procedimentos, Métodos e Padrões de TI;
- Inexistência de uma metodologia para implementação do portfólio de projetos;
- Inexistência de uma metodologia para gerenciamento de programas/projetos;
- Falta do conhecimento prático em gerenciamento de projetos para concepção e execução do Plano de Projeto;
- Falha no desenvolvimento dos Projetos devido à falta de envolvimento das partes interessadas, conhecimento técnico e levantamento de requisito insuficiente;
- Retrabalho em Projetos devido ao escopo mal definido;



- Inexistência de uma metodologia para gerenciamento de demandas;
- Estrutura Organizacional da TI não atende necessidades Corporativas;
- Falta a prática de Planejamento, Gestão de Projetos, Padrões, Métodos e Procedimentos em TI;
- Existência de estruturas de TI fora da localização física da área da DTIN e que atuam de forma independentes;
- Estrutura de TI e localização física da área da DTIN inadequada para o atendimento ao ON;
- Estrutura subdimensionada para as futuras demandas de TI;
- Sobreposição de funções e responsabilidades da TI na instituição;
- Envolvimento das Chefias no nível operacional compromete a gestão do nível tático e estratégico;
- Falta de visão de integração entre os processos dos frameworks adotados;
- Falta de visibilidade dos Benefícios da TI para justificar esforços das equipes;
- Falta de visibilidade dos projetos que estão sendo executados na TI;
- Inexistência de esquema de classificação de dados aplicado em toda a instituição, baseado na criticidade e sensibilidade (p.ex. publico, confidencial, muito secreto);
- Ausência de um Catálogo de Serviços que contemple a visão dos serviços de negócios, serviços técnicos e componentes de TI;
- Ausência de definição do Responsável pelo Serviço;
- Processo de Gerenciamento Configuração e Ativo de Serviço não implementado com visão corporativa, comprometendo a análise de riscos e priorização de incidentes graves;
- Comunicação não estruturada, informal e mal gerenciada entre departamentos afetando as atividades de TI;
- Não se aplicam métodos para gerenciamento de risco, entretanto existe iniciativa para contratação de plano para continuidade do negócio;
- Não existe cultura de planejamento para aquisições;
- Inexistência de processo estabelecido para desenvolvimento de plano de arquitetura da informação;



- Inexistência de processo estabelecido para desenvolvimento de plano de infraestrutura de tecnologia;
- Ausência de um processo definido para monitorar o desempenho da TI;
- Ausência de um processo definido para gerenciar incidentes, requisições de serviços, problemas e mudanças;
- Ausência de um processo definido para gerenciar eventos e acessos;
- Ausência de um processo definido para gerenciar níveis de serviço;
- Ausência de um processo definido para gerenciar desempenho e capacidade de TI;
- Ausência de um processo definido para gerenciar disponibilidade e continuidade de TI;
- Ausência de um processo definido de Planejamento da transição, Conhecimento, Liberação e Distribuição, Teste e Validação e Avaliação;
- Falhas na Segurança da Informação;
- Ausencia de padrões de hardware e software.
- Visão dos Clientes e Usuários de o que a TI deve prover não é uniforme.

□ OPORTUNIDADES

- Acesso as melhores práticas de mercado;
- Uso de modelos e ferramentas pré-avaliados;
- Utilização de Novas Tecnologias;
- Status QUO (Autonomia para especificar e adquirir tecnologia);
- Utilização do Apoio da Alta Administração para implementar as mudanças estratégicas.

□ AMEAÇAS

- Altos custos com consultorias externas;
- Taxas de Obsolescência da Tecnologia;



- Demandas novas e com volumes crescentes não suportados pelas plataformas existentes;
- Dependência critica de prestadores de serviços;
- Exigências de controle interno atendidas com menor qualidade, maior custo e extrema dependência de pessoas;
- Dificuldade na retenção e rotatividade de pessoal capacitado e habilitado;
- Desvios de Escopo, Prazo e Custos de Projetos comprometendo a imagem da TI;
- Redução Orçamentária;



O Diagnóstico é apresentado nos 4 temas a seguir de forma a permitir o foco necessário.

- **DIAGNÓSTICO GOVERNANÇA DE TI (PROCESSOS ESTRATÉGICOS)**
- **DIAGNÓSTICO GESTÃO DE PROJETOS E PROCESSOS DE TI (PROCESSOS TÁTICOS E OPERACIONAIS)**
- **DIAGNÓSTICO SERVIÇOS, SISTEMAS E APLICATIVOS**
- **DIAGNÓSTICO DE RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO**

4.1. DIAGNÓSTICO GOVERNANÇA DE TI (PROCESSOS ESTRATÉGICOS)

A Governança de TI tem como objetivo primordial definir, com base nas necessidades do negócio, o que TI deve fazer. A adequada Governança permite a alta administração tomar as melhores decisões, assegurar serviços e funcionalidades e proteger os recursos de TI.

É responsabilidade da Governança assegurar que:

1. TI preste os serviços alinhados com as estratégias institucionais;
2. TI e as novas tecnologias sejam utilizadas para introduzir inovações em processos, produtos/serviços e melhorar o desempenho organizacional;
3. Os serviços e as funcionalidades sejam oferecidos com a maior eficácia de custos e de maneira mais eficiente possível;
4. Todos os riscos de TI sejam conhecidos e que seus recursos (informações, sistemas, equipamentos, etc.) estejam seguros.



4.1.1. DIAGNÓSTICO MISSÃO E VISÃO DA TI

Ausência de processo formal que estabeleça o envolvimento da alta administração na seleção, priorização, aprovação, planejamento, estudos de viabilidade e acompanhamento dos projetos de TI da instituição.

O planejamento estratégico aprovado pela Alta Administração, não define claramente a atuação de TI na instituição e os papéis e responsabilidades dos usuários no processo.

4.1.2. DIAGNÓSTICO PLANEJAMENTO ESTRATÉGICO DE TI ALINHADO AOS OBJETIVOS DE NEGÓCIO

Ausência de planejamento estratégico de TI alinhado com os objetivos estratégicos e metas institucionais.

A priorização das necessidades das áreas é realizada de forma independente, sem consideração das metas e objetivos organizacionais;

4.1.3. DIAGNÓSTICO ESTRATÉGIA E PADRÕES TECNOLÓGICOS

Ausência de um processo que determine as diretrizes tecnológicas assegurando sistemas, aplicativos, recursos e capacidade padronizada, integrada, estável, com boa relação custo-benefício que atenda os requisitos atuais e futuros do negócio.

Terceirização não envolve o desenvolvimento de aplicativos sob gestão da DTIN;

Processos deficientes de especificação de serviços, contratação, acompanhamento dos serviços e gestão das entregas.

O contrato atual não obedece os princípios da IN04.

4.1.4. DIAGNÓSTICO ESTRUTURA ORGANIZACIONAL DE TI

A instituição de TI não responde as mudanças de forma proativa e não contempla todos os papéis necessários para atender as áreas de negocio.

Ausência de um processo formal para gerenciamento de recursos humanos de TI.

Situação referente a recursos humanos qualificados em TI na DTIN/ON é extremamente crítica.



4.1.5. ARQUITETURA DA INFORMAÇÃO EMPRESARIAL

Ausência de um processo para definir a Arquitetura da Informação que satisfaça ao requisito do negócio para a TI, com agilidade na resposta aos requisitos, fornecendo informação confiável e consistente e integrando completamente as aplicações aos processos de negócio.

Ausência de um modelo de informação da instituição que permita o desenvolvimento de aplicações e atividades de apoio à decisão consistente com os planos de TI. O modelo não facilita a criação, o uso e o compartilhamento otimizados da informação pelo negócio para manter a integridade e ser flexível, funcional, com boa relação custo-benefício, rápido, seguro e resistente a falhas.

4.1.6. VISÃO DA ESTRATÉGIA DOS SERVIÇOS

Os projetos são selecionados e priorizados sem considerar critérios organizacionais, considerar critérios organizacionais, executados sem o adequado envolvimento de todos os interessados internos e externos da instituição (stakeholders).

Ausência de ferramenta que apoie a elaboração do BSC e priorização do portfólio de projetos.

Ausência de processo e ferramentas para justificar e ratear custos dos serviços de TI. Ausência de processo definido para gerenciar demanda conforme capacidade dos ativos estratégicos.

4.1.7. MELHORIA DOS SERVIÇOS

Ausência de metodologia e processo a serem seguidos para avaliar a entrega de soluções e serviços de TI e monitorar a contribuição da TI para os resultados do negócio.



4.2. DIAGNÓSTICO GESTÃO DE PROJETOS E PROCESSOS DE TI (PROCESSOS TÁTICOS E OPERACIONAIS)

A Gestão de Projetos e Processos de TI tem como objetivo primordial a gestão dos recursos humanos, tecnológicos e os processos necessários para implementar e operar projetos aprovados (como fazer). A boa gestão cria condições para que TI ofereça soluções de qualidade e com cumprimento dos prazos e custos acordados.

4.2.1. GESTÃO DE PROJETOS DE TI

Projetos de TI executados sem o tratamento adequado do escopo e dos riscos inerentes ao porte dos projetos, sem o adequado envolvimento de todos os interessados internos e externos da instituição (stakeholders).

Existência de soluções em operação com potencial de aproveitamento das informações e dados não utilizados amplamente pelos usuários. Existência de usuários com baixo conhecimento para definir e especificar aplicações e serviços para TI, bem como gerenciar a execução dos mesmos pela área usuária.

Apesar da existência do papel do “GESTOR DE SISTEMAS”, ou seja, usuário responsável por cada sistema, visando o estabelecimento dos requerimentos, apoio aos projetos e serviços, homologação dos produtos , não existe processo formal que defina os papéis e responsabilidades.

Apesar da existência do papel do “GESTOR DE SISTEMAS”, ou seja, usuário responsável por cada sistema, visando o estabelecimento dos requerimentos, apoio aos projetos e serviços, homologação dos produtos , não existe processo formal que defina os papéis e responsabilidades.

Na ferramenta de projetos instituída pelo MCT não contempla a gestão de todos os projetos em execução pela instituição.

4.2.2. GESTÃO DE PROCESSOS DE TI

Ausência de um processo de Gerenciamento do Catálogo de Serviço que descreva os serviços oferecidos por TI para instituição.
Ausência de ferramenta que apoie o processo.



Desconhecimento pelos usuários dos serviços de TI oferecidos pela DTIN.

O processo desenvolvimento de acordos de nível de serviço não foi estabelecido com pontos de verificação para reavaliação dos níveis de serviço e satisfação do cliente.

Ausência de ferramenta que apoie os processos. Desconhecimento dos clientes e usuários dos níveis de atendimento dos serviços de TI.

O processo de Gerenciamento de Capacidade não foi estabelecido comprometendo a avaliação de capacidade de Negocio, do Serviço e dos Componentes. O processo de Gerenciamento de Disponibilidade não está definido.

Apesar de estarem disponíveis ferramentas para monitoramento de rede, recursos computacionais ou de serviços, não foi identificado uma regulariedade da atividade.

O processo de Gerenciamento de Mudança no ambiente de TI do ON não está definido. O processo de Gerenciamento de Fornecedores não está definido. O processo de Gerenciamento de Configuração e Ativos do Serviço não está definido.

Apesar de estarem disponíveis ferramentas para gerenciamento da configuração e ativos, o parque de equipamentos não está configurado para que possam ser identificados.

Os processos de Gerenciamento de Conhecimento, Gerenciamento de Liberações e implantação, Teste e Validação não está definido, Planejamento da Transição e Suporte e de Avaliação não estão definidos.

O processo de Gerenciamento de Incidentes foi definido de forma básica necessitando ser ampliado e integrado com os demais processos de gerenciamento de serviços;

Não há garantia de que todos os incidentes foram registrados.

4.2.3. CENTRAL DE SERVIÇOS

Não existe uma central de serviços e não é possível assegurar que todos os incidentes são registrados.

4.2.4. GERENCIAMENTO DAS APLICAÇÕES



Ausência de metodologia para suporte ao ciclo de vida de gerenciamento das aplicações para projetos de grande impacto, prazos e custo não é a mais adequada.

Soluções e controles elaborados pelas áreas com utilização de planilhas e softwares não homologados por TI.

Sistemas especialistas desenvolvidos e mantidos em linguagens distintas e descontinuadas pelas áreas departamentais.

Não atendimento a sistemas especialistas. Não existe codificação estruturada.

Usuários com conhecimento insuficiente para definir e implantar soluções departamentais que ofereçam segurança.

4.2.5. GERENCIAMENTO DE OPERAÇÕES

Deficiência nos processos de planejamento, execução e controle dos sistemas em produção. Ferramentas não definidas.

4.2.6. GERENCIAMENTO TÉCNICO

Deficiência na gestão do ambiente de infraestrutura. Ausência de recursos capacitados o suficiente, atualizados em soluções para o negócio e preparados para apoiar as atividades fins do ON em que esteja envolvida a Tecnologia da Informação;

4.3. DIAGNÓSTICO SERVIÇOS, SISTEMAS E APLICATIVOS

A Dimensão de Serviços Prestados trata de questões relativas que atendem os clientes internos e externos, englobando o desenvolvimento / utilização / manutenção de sistemas aplicativos e dos sites Internet/Intranet, utilização dos serviços de correio eletrônico (QMAIL), das ferramentas de colaboração (GED, Workflow, escritório), soluções especialistas (área de Astronomia, Geofísica, Data Warehouse, Data Mart, etc) e soluções administrativas.

4.3.1. SISTEMAS DE USO CORPORATIVO

SIGTEC – Sistema de Informações Gerenciais e Tecnológicas



SCDP - Sistema de Concessão de Diárias e Passagens

Atendem parcialmente a gestão dos recursos financeiros, gestão de competências, acompanhamento de indicadores e projetos.

Compartilhamento de uma base de dados única, administrada pelo Gestor Central do Ministério do Planejamento. Não existe garantia de disponibilidade. Falta de integração com outros sistemas de informação. Há necessidade de integração com um sistema administrativo do ON.

4.3.2. DIVISÃO ADMINISTRATIVA - SERVIÇO DE RECURSOS HUMANOS

O SRH tem como atribuição, coordenar, supervisionar e executar todas as atividades referentes a recursos humanos tais como: admissão, concursos, treinamento, estágios, avaliação de desempenho, aposentadoria, pensão, demissão, exoneração, afastamento do país, férias, folha de pagamento, assistência médica e social e operacionalização dos sistemas instituídos pelo Governo Federal de Administração de Recursos Humanos- SIAPE e o de Apreciação de Atos - SISAC.

SIAPE e SIAPENET - SISTEMA INTEGRADO DE ADMINISTRAÇÃO DE RECURSOS HUMANOS

SISACNET - REGISTRO E APRECIAÇÃO DE ATOS DE ADMISSÃO E CONCESSÃO

SIAPECAD - SISTEMA DE CADASTRO DETALHADO DE SERVIDORES

Sem garantia de disponibilidade, comprometendo a integridade dos dados e não atendendo as necessidades corporativas.

SISTEMA DE RH (em processo de descontinuidade)

Base de dados com registros não disponíveis no SIAPE

GESTÃO DE DESEMPENHO

Falta de aplicativo para suportar de forma otimizada o processo.

4.3.3. DIVISÃO ADMINISTRATIVA - SERVIÇO FINANCEIRO

O SEF tem como atribuição, coordenar, supervisionar e executar todas as atividades no que se refere a recursos orçamentários e financeiros, balanço, prestação de contas, repasses, emissão de empenhos, pagamentos, contabilização, tudo através da operacionalização do sistema instituído pelo Governo Federal - SIAFI, registro, acompanhamento e controle de Convênios, Auxílios e Contratos.

SIAFI - SISTEMA INTEGRADO DE ADMINISTRAÇÃO FINANCEIRA DO GOVERNO FEDERAL

Sem garantia de disponibilidade, comprometendo a integridade dos dados e não atendendo as necessidades corporativas.

4.3.4. DIVISÃO ADMINISTRATIVA - SERVIÇO DE MATERIAL E PATRIMÔNIO

O SMP tem como atribuição, coordenar, supervisionar e executar todas as atividades que envolvam compras, licitação, convênios, contratos, almoxarifado, patrimônio e a operacionalização do SICAF - Sistema de Cadastro de Fornecedores do Governo Federal e SIDEC.

SICAFWeb - SISTEMA DE CADASTRAMENTO UNIFICADO DE FORNECEDORES

SIASG - SISTEMA INTEGRADO DE ADMINISTRAÇÃO DE SERVIÇOS GERAIS

Atende as necessidades

GESTÃO DE PATRIMÔNIO

Versão Beta do SIGTEC incorpora um módulo de patrimônio que encontra-se em fase de teste.

GESTÃO DE FORNECEDORES

Realizado através do SIGTEC e dos sistemas disponíveis para administração pública. Atende parcialmente.



GESTÃO DE CONTRATOS

Não existe um sistema que apoie a gestão de contratos. Controle realizado manualmente.

4.3.5. DIVISÃO ADMINISTRATIVA - SERVIÇO DE APOIO LOGÍSTICO

O SAL tem como atribuição, coordenar, supervisionar e executar todas as atividades necessárias a conservação e manutenção das instalações e do patrimônio do ON, bem como os serviços de vigilância, gráfica, xerox, telefonia, portaria, veículos e operacionalização do SICAF - Sistema de Cadastro de Fornecedores do Governo Federal

GESTÃO DO ALMOXARIFADO DEPARTAMENTAL

Não existe integração com o sistema de controle de almoxarifado central do ON.

SISTEMAS ADMINISTRATIVOS

Não utilização dos recursos disponíveis nos sistemas administrativos.

GESTÃO DE FROTA

Inexiste um controle de gestão de frota apoiado por um sistema automatizado.

4.3.6. DIVISÃO DE INFORMAÇÕES E DOCUMENTAÇÃO

Atende as necessidades da área.

4.3.7. COORDENAÇÃO DE ASTRONOMIA E ASTROFÍSICA

PROGRAMAS DE PESQUISA



Exposição ao risco com a utilização de linguagens de programação que estão sendo descontinuadas e/ou sem suporte adequado. (Turbo Pascal, Visual Basic, Delphi, Borland C), Não estando documentado e conhecimento centralizado em um único colaborador;

Máquinas servidoras encontram-se fora do DATA CENTER corporativo, não atendendo os padrões de controle e segurança para os recursos de TI do ON;

Três recursos terceirizados suportam as atividades de manutenção, não subordinação ao gestor do contrato de terceirização;

Padrões existentes desenvolvidos pela equipe sem apoio do DTIN;

Utilização de serviço de e-mail próprio, não utilizando o e-mail corporativo.

SOFTWARE ESPECIALISTAS

Número de licenças não atende a demanda

4.3.8. GRUPO DE PESQUISA EM ASTRONOMIA - GPA

Desconhecimento pela DTIN das necessidades e sistemas desenvolvidos pela área.

Máquinas servidoras encontram-se fora do DATA CENTER corporativo, não atendendo os padrões de controle e segurança para os recursos de TI do ON.

Três recursos terceirizados suportam as atividades de manutenção e não subordinação ao gestor do contrato de terceirização.

Padrões existentes desenvolvidos pela equipe sem apoio do DTIN.

Utilização de serviço de e-mail próprio, não utilizando o e-mail corporativo.

Não existência de registro de avaliações de segurança da rede interna realizadas pelo DTIN.

4.3.9. COORDENAÇÃO DE GEOFISICA

PROGRAMAS DE PESQUISA



Exposição ao risco com a utilização de linguagens de programação que estão sendo descontinuadas e/ou sem suporte adequado. (Turbo Pascal, Visual Basic, Delphi, Borland C). Não apresentando documentação.

Os programas necessários a pesquisa são desenvolvidos e armazenados em estações de trabalho que não atendem aos procedimentos e padrões de segurança.

4.3.10. DIVISÃO DE PÓS-GRADUAÇÃO

SOFTWARE ESPECIALISTAS

Utilização de softwares não homologados pela TI. Não utiliza padrões corporativos para aquisição de hardware e softwares com base em estudo de viabilidade. Utilização de áreas de armazenamento sem controle ou segurança com relação ao conteúdo armazenado.

4.3.11. DIVISÃO DE SERVIÇO DA HORA

SISTEMA DE GARANTIA DA QUALIDADE E CALIBRAÇÃO

REDE DE SINCRONISMO

REDE DE CARIMBO DE TEMPO

DIFUSÃO DA HORA

Realização de atividades sob a responsabilidade da DTIN. A realização do backup está a cargo da própria área.

Versão do S.O. não oferece segurança. O suporte fornecido pelo DTIN é considerado deficiente. O executável encontra-se instalado nas próprias estações. A documentação do sistema de gestão encontra-se disponível na arvore de diretórios sem a segurança adequada. Não existência de registro de avaliações de segurança da rede interna realizadas pelo DTIN.

Inexistência de padrões corporativos para desenvolvimento, homologação, teste e deploy em ambiente de produção.



Utilização de linguagens de programação que estão sendo descontinuadas e/ou sem suporte adequado. (Turbo Pascal, Visual Basic, Delphi, Borland C). Não documentado. Conhecimento centralizado em um único colaborador.

Os servidores provedores do serviço encontram-se fora do DATA CENTER corporativo, não atendendo os padrões de segurança do ON.

SITE – HORA LEGAL BRASILEIRA

Não é mantido pelo DTIN; Não está no domínio do site institucional <http://www.horariodebrasilia.org/>
Não está documentado.

4.3.12. DIVISÃO DE ATIVIDADES EDUCACIONAIS

ENSINO A DISTÂNCIA

Inexistência de padrões de avaliação de disponibilidade e capacidade de rede.

SITE OFICIAL DA INSTITUIÇÃO

Inexistência de padrões corporativos para desenvolvimento, homologação, teste e deploy em ambiente de produção.
Não documentado. Falta de padronização nas fontes utilizadas. Navegabilidade prejudicada devido ao grande número de links que abrem novas sessões. Falta de processo definido para autorização de mudanças no conteúdo. Falta de controle de mudanças e demandas. Ambiente de desenvolvimento não se encontra sob a supervisão da DTIN.

4.4. DIAGNÓSTICO DE RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO



A Dimensão de Recursos Tecnológicos e Segurança da Informação tratam de questões relativas à arquitetura de recursos de TI, que abrange todos os equipamentos de informática, os programas que permitem operar os equipamentos de informática e desenvolver sistemas, os programas de uso geral (ex.: editores de texto, planilhas eletrônicas, correio eletrônico, etc.), estrutura de telecomunicações e rede de computadores, bem como as questões relativas à Segurança da Informação, segundo uma ótica de continuidade de negócios, considerando não somente o aspecto de confidencialidade das informações como também de sua integridade e disponibilidade.

Foram identificados os seguintes pontos de alerta:

Ausência de um processo de gestão de segurança da informação.

Ausência de cultura de gerenciamento de riscos.

Ausência de um processo formal de auditoria para assegurar o cumprimento, por TI, de políticas, normas e procedimentos considerados essenciais para a continuidade das operações da instituição.

Ausencia de uma Política de Segurança. Identificação deficiente dos ativos e a sua importância para a Instituição

Deficiência no processo de tratamento de incidentes de segurança. O processo de Gerenciamento de Continuidade não está definido Ausência de uma politica de backup que assegure a continuidade do negócio. Deficiência documentacional e de capacitação.

Deficiência nos controles de segurança física. O processo de Gerenciamento de Acesso não foi definido. Configuração de segurança dos servidores inadequada. Diversas versões instaladas sem atualização e contrato de suporte com fornecedor.

Ambiente tecnológico sem padrão e sem domínio da DTIN. Deficiência na política de acesso à internet.

Ausência de documentação/Informação sobre segurança na intranet. Configurações de segurança nas estações de trabalho deficientes e diversos Sistemas Operacionais sem controle de licenças e atualização. Deficiência na documentação e domínio das configurações dos diversos elementos fierewaal/rotedores colocados na rede do ON. Deficiência das ferramentas de análises e detecção de ataques.



5. RECOMENDAÇÕES

As recomendações apresentadas através das ações detalhadas no item 7 – PLANO DE PROJETOS estão resumidas nas seguintes proposições:

5.1. GOVERNANÇA DE TI

Cuidar da governança e do processo de contratação como forma de garantir que as soluções de TI sejam adequadas aos problemas que tentam resolver, considerando a tecnologia existente no mercado e com os menores custos possíveis, dado o aparato legal. Desta forma a implantação de um Comitê de TI permitirá o alinhamento estratégico das ações de TI as necessidades de negócio da organização.

Necessidade de adequação do contrato atual de terceirização a luz da IN 04.

Capacitação do corpo técnico do ON para prover os serviços necessários a instituição.

5.2. GESTÃO DE PROJETOS E PROCESSOS DE TI

Estabelecer a cultura de projetos de TI através da implantação de uma metodologia que suporte o estudo de viabilidade, detalhamento dos requisitos, acompanhamento e controle dos projetos de TI.

A estruturação de um núcleo dedicado aos projetos de TI incorporado no Escritório de Governança e integrado à área de relacionamento dos clientes torna-se um fator crítico para a aplicação dos métodos de gerenciamento de projetos de TI.

Estabelecimento de uma central de serviços que venha a permitir a melhoria do atendimento, suporte aos níveis de serviços de TI acordados e o controle das demandas de serviços de TI oferecidos a instituição.

Melhoria dos controles internos relacionados ao catálogo de serviços e níveis de serviços (evoluindo para um portfólio de serviços), a adequada mensuração do esforço de desenvolvimento, antes, durante e depois da construção do serviço, em todas as fases do ciclo de desenvolvimento, de modo a se construir uma indicadores da produtividade dos serviços técnicos alocados e se poder realizar benchmarking, comparando-se os índices locais com outras organizações/empresas.



5.3. SERVIÇOS, SISTEMAS E APLICATIVOS

Modernização dos sistemas existentes e desenvolvimento dos novos sistemas previstos no PDTI através do desenvolvimento de estudos para contratação de serviços de desenvolvimento de software por empresas especializadas para as quais possam ser direcionadas as novas demandas. Torna-se, portanto, oportuna a adoção e criação de uma infraestrutura de desenvolvimento, inclusive a adoção de uma metodologia de desenvolvimento de sistemas, que permita a gestão do desenvolvimento de sistemas.

Centralização na área responsável pela TI do ON da gestão do desenvolvimento dos serviços de intranet e extranet institucionais do ON, ficando a responsabilidade pela gestão e manutenção do conteúdo dos sites institucionais a cargo da área especializada da instituição.

Otimização da capacidade de processamento e armazenamento através da centralização dos recursos hoje existentes em toda a instituição, dispondo desta forma de um ambiente seguro.

5.4. RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO

O sucesso do ambiente central de operações e de rede é incluir, alterar, melhorar ou excluir completamente os métodos de trabalho (hoje apenas reativos aos eventos), para métodos preventivos que possibilitem construir um ambiente central e de redes compatíveis com a necessidade das áreas.

A necessidade de estabelecer critérios claros para a modernização do parque computacional, como a atualização do parque computacional com idade mínima de 3 anos e máxima de 5 anos, ou mesmo a renovação a cada ano de 1/3 do parque, em especial na camada cliente, sempre adquirindo equipamentos novos com no mínimo três anos de garantia. Desse modo, em três anos, todo o parque estará atualizado e coberto por garantia.

contratação de

Realização periódica de serviço especializado voltado a área de auditoria em Segurança da Informação com o uso das melhores práticas, como a Norma ISO 27.001 e 27.002 e sucessoras e estruturas de controle de mercado, implantando práticas e ferramentas modernas aplicadas à segurança da informação.



A avaliação, manutenção e aquisição de novos equipamentos através de contratos de garantia, manutenção e suporte para todos os ativos da rede de todo o ON incluindo: os ambientes centrais de processamento, ambientes de serviços de arquivos das unidades descentralizadas, software, equipamentos servidores de rede, sistemas de armazenamento (storage), mecanismos de proteção e sistemas de controle de intrusão (IPS, firewall, proxys e antivírus), entre outros.

Estruturar adequadamente um ambiente central de operações contingenciado.



6. PRIORIDADE DOS PROJETOS

Este item contempla a prioridade dos projetos a serem executados na Onda 1, Onda 2 e Onda 3

Considerando o volume e a complexidade dos problemas identificados, as ações propostas foram ordenadas em 3 ondas:

1ª. Onda – duração 8 meses - **ações emergenciais e as de curto prazo** (de Maio/2011 a Dezembro/2011) visando criar condições básicas para o início da implementação da Governança.

2ª. Onda – duração 24 meses - ações que deverão ser deflagradas de Janeiro/2012 a Dezembro/2013, visando reforçar as condições para maior eficiência / eficácia de TI.

3ª. Onda – duração 24 meses - ações que deverão ser deflagradas de Janeiro/2014 a Dezembro/2015, visando melhorar nível de serviços aos clientes internos e externos e da segurança.

Nesta etapa foram destacadas as principais **ações de curto prazo** visando à correção de problemas e ajustes necessários para o fortalecimento da Divisão de Tecnologia da Informação – DTIN do Observatório Nacional - ON.



6.1. 1ª ONDA - AÇÕES DE CURTO PRAZO

1ª. Onda – duração 8 meses - **ações emergenciais e as de curto prazo** (de Maio/2011 a Dezembro/2011) visando criar condições básicas para o início da implementação da Governança.

6.1.1. GOVERNANÇA DE TI

1ª ONDA	Nº	GOVERNANÇA DE TI	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	MISSÃO E VISÃO DE TI - ESTABELECER PROCESSO DE PLANEJAMENTO E ACOMPANHAMENTO PERIÓDICO, PELA ALTA ADMINISTRAÇÃO, DOS PROJETOS RELEVANTES DE TI (vide Anexo I).	Alta Administração	Alta Administração	Mai/11	Imediato	Internos	-
	2	GRUPO EXECUTIVO DE TI - ADEQUAR O ATUAL COMITÊ, "GRUPO EXECUTIVO DE TI - GETI" COMPOSTO PELOS GERENTES DOS PRINCIPAIS DEPARTAMENTOS E USUÁRIOS CADA DEPARTAMENTO, VISANDO RECOMENDAR À ALTA ADMINISTRAÇÃO POLÍTICAS E PROJETOS DE TI (vide Anexo I).	Alta Administração	Alta Administração	Mai/11	Imediato	Internos	-

OZ	Nº	GOVERNANÇA DE TI	RESPONS.	RESPONS.	DATA	DURAÇÃO	RECURSOS	CUSTO
----	----	------------------	----------	----------	------	---------	----------	-------



		AÇÕES	PROPOR	APROVAR	INÍCIO			(R\$ mil)
	3	<p>PARTICIPAÇÃO DOS USUÁRIOS NA GOVERNANÇA DE TI - DEFINIR REGRAS E PROCEDIMENTOS <i>EMERGENCIAS</i> PARA NORTEAR O PROCESSO DE DESENVOLVIMENTO E MUDANÇAS DAS SOLUÇÕES E SERVIÇOS DE TI, E QUE ESTABELEÇAM:</p> <ul style="list-style-type: none"> • PAPEL E RESPONSABILIDADES DOS USUÁRIOS, AUDITORIA E TI; • NECESSIDADE DE ESTUDO DE VIABILIDADE DOS NOVOS PROJETOS (ANTEPROJETO); • APROVAÇÃO DAS ESPECIFICAÇÕES FUNCIONAIS PELOS USUÁRIOS; • ACOMPANHAMENTO RIGOROSO DOS PROJETOS; • HOMOLOGAÇÃO DOS SERVIÇOS ANTES DE ENTRAREM EM OPERAÇÃO. 	TI	GETI Alta Administração	Jun/11	3m	Internos	-
	4	PADRÕES TECNOLÓGICOS - ESTABELECER E DIVULGAR O PADRÃO DE SOFTWARE E HARDWARE A SER UTILIZADO NA EMPRESA PARA ESTAÇÕES E SERVIDORES ATRAVÉS DE PORTARIA INTERNA.	TI	GETI	Jun/11	Imediato	Internos	-
	5	PALESTRA PARA ALTA ADMINISTRAÇÃO – EFETUAR PALESTRAS PARA A ALTA ADMINISTRAÇÃO VISANDO MELHORAR O ENTENDIMENTO SOBRE A GESTÃO E GOVERNANÇA DE TI (vide ANEXO 13).	TI	TI	Jun/11	Continuo	Internos	-
	6	PALESTRA PARA USUÁRIOS E TI – EFETUAR PALESTRAS E PROGRAMAS DE TREINAMENTO PARA TI E USUÁRIOS VISANDO MELHORAR: A COMUNICAÇÃO, A APRECIAÇÃO DE TI E A DIVULGAÇÃO DAS METAS INSTITUCIONAIS (vide ANEXO 13).	TI	TI	Jun/11	Continuo	Internos	-



1ª ONDA	Nº	GOVERNANÇA DE TI	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	7	PROCESSO PARA SOLICITAÇÃO DE MUDANÇAS – IMPLEMENTAR PROCESSO BÁSICO PARA A SOLICITAÇÃO, PLANEJAMENTO, EXECUÇÃO, ACEITAÇÃO E ACOMPANHAMENTO DAS MUDANÇAS DE SISTEMAS E DE HARDWARE SOLICITADAS A TI PELOS USUÁRIOS.	TI	TI	Jul/11	3m	Internos	-
	8	GRUPO DE GESTÃO DE MUDANÇAS – CRIAR O GRUPO DE GESTÃO DE MUDANÇAS E NOMEAR OS SEUS MEMBROS ATRAVÉS DE PORTARIA INTERNA VISANDO AVALIAR O IMPACTO DAS MUDANÇAS EM SISTEMAS APLICATIVOS, RECOMENDAR A SUA EFETIVAÇÃO E A PRIORIDADE. (vide ANEXO 13).	TI	TI	Jul/11	3m	Internos	-
	9	ADEQUAR ESTRUTURA ORGANIZACIONAL – IMPLEMENTAR OS AJUSTES PLANEJADOS DE ACORDO COM A IN4.	TI	TI	Jul/11	3m	Internos	-
	10	TERCEIRIZAÇÃO DE SERVIÇOS E ANS – ESTABELECER E INCLUIR NOS CONTRATOS “ACORDO DE NÍVEL DE SERVIÇOS” (<i>SERVICE LEVEL AGREEMENT</i> SLA - METAS DE DESEMPENHO E CRITÉRIOS DE AVALIAÇÃO DOS SERVIÇOS PRESTADOS) PARA OS PRINCIPAIS SERVIÇOS TERCEIRIZADOS EM TI DE ACORDO COM A IN4.	TI	GETI Alta Administração	Jul/11	3m	Internos	-
	11	CAPACITAÇÃO GERENCIAL DOS GESTORES DE TI E USUÁRIOS GESTORES – PARTICIPAÇÃO DOS GESTORES EM PROGRAMAS DE DESENVOLVIMENTO GERENCIAL GESTÃO / GOVERNANÇA DE SERVIÇOS DE TI, COM FOCO EM PLANEJAMENTO DAS ATIVIDADES DA ÁREA.	TI	TI	Jul/11	3m	Externos	-
	12	CAPACITAÇÃO TÉCNICA DOS PROFISSIONAIS DE TI – IDENTIFICAR NECESSIDADES E REALIZAR PROGRAMAS DE APERFEIÇOAMENTO/ ATUALIZAÇÃO TÉCNICA DOS TÉCNICOS DE TI.	TI	TI	Jul/11	6m	Externos	-



6.1.2. GESTÃO DE PROJETOS E PROCESSOS

1ª ONDA	Nº	GESTÃO DE PROJETOS E PROCESSOS DE TI	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
1ª ONDA	1	GERÊNCIA DE PROJETOS – CRIAR METODOLOGIA BÁSICA, IMPLANTAR E CAPACITAR TI E USUÁRIOS EM GERÊNCIA DE PROJETOS DE TI, VISANDO INICIAR A SUA PRÁTICA. – (vide ANEXO 6).	TI	GETI	Jun/11	3m	Interno	-
	2	INDICADORES DE DESEMPENHO OU MÉTRICAS - DEFINIR INDICADORES PARA MEDAÇÃO DO DESEMPENHO DA DTIN COM BASE NO FRAMEORK COBIT	TI	GETI	Jul/11	1m	Interno	-
	3	PREPARAR ESTUDO PARA ADOÇÃO E PADRONIZAÇÃO - FERRAMENTAS INTEGRADAS PARA GERENCIAMENTO DO AMBIENTE DE TI – OPEN SOURCE	TI	TI	Jul/11	1m	Interno	-
	4	GESTÃO DE SISTEMAS - ADOTAR E IMPLANTAR METODOLOGIA BASICA DE DESENVOLVIMENTO DE SISTEMAS.	TI	GETI	Jul/11	3m	Externo	-
	5	MELHORIA – APRIMORAR OS PROCEDIMENTOS DE MANUTENÇÃO PREVENTIVA DOS EQUIPAMENTOS.	TI	TI	Jul/11	1m	Interno	-
	6	ELABORAR E IMPLANTAR - PLANO DE CONTINUIDADE DO NEGÓCIO PARA STORAGE	TI	TI	Jul/11	1m	Interno	-



6.1.3. SERVIÇOS, SISTEMAS E APLICATIVOS

1ª ONDA	Nº	SERVIÇOS, SISTEMAS E APLICATIVOS	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
1	1	DEFINIR ESTUDO E ELABORAR PROJETO - DENSENVOLVIMENTO DE SISTEMA INTEGRADO DE GESTÃO PARA O OBSERVATÓRIO NACIONAL INTEGRADO AOS SISTEMAS GOVERNAMENTAIS.	TI	TI	Imediato	2m	Interno	-
	2	DEFINIR ESTUDO E ELABORAR PROJETO - UNIFICAÇÃO E MELHORIAS NO SITE INSTITUCIONAL, DE MODO A ATENDER AS NECESSIDADES DE DIVULGAÇÃO E INCORPORAÇÃO DOS DEMAIS SITES NÃO PADRONIZADOS.	TI	TI	Imediato	2m	Interno	-
	3	REALIZAR ESTUDO DE VIABILIDADE - ADOÇÃO DE NOVA SOLUÇÃO DE ENSINO A DISTÂNCIA.	TI	TI	Out/11	2m	Interno	-
	4	DEFINIR ESTUDO E ELABORAR PROJETO - LEVANTAMENTO DOS REQUISITOS PARA MODERNIZAÇÃO DOS SISTEMAS DE APOIO AS ATIVIDADES DA DSHO.	TI	TI	Imediato	2m	Interno	-
	5	DEFINIR ESTUDO E ELABORAR PROJETO - LEVANTAMENTO DOS REQUISITOS PARA COMPARTILHAMENTO CORPORATIVO DE PROCESSAMENTO E ARMAZENAMENTO.	TI	TI	Out/11	2m	Interno	-



	6	IDENTIFICAR SOLUÇÃO PARA CONTROLE DE FROTA DE VEICULOS PERTENCENTES A INSTITUIÇÃO	TI	TI	Out/11	1m	Interno	-
	7	IDENTIFICAR REQUISITOS – NECESSÁRIOS PARA A INCORPORAÇÃO DO MODULO DE CONTROLE DE PATRIMONIO	TI	TI	Out/11	1m	Interno	-



6.1.4. RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO

1ª ONDA	Nº	RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
1	1	POLITICA DE SEGURANÇA - IMPLANTAR A POLÍTICA DE SEGURANÇA COM ENFASE NO ITEM SEGURANÇA LÓGICA DA INFORMAÇÃO (CONTROLE DE ACESSO, SENHAS, ESTAÇÕES, ACESSO A INTERNET, SEGURANÇA PERIMETRAL, MONITORAÇÃO DE ACESSO A SISTEMAS, CRIPTOGRAFIA, ANTI-VIRUS, GERENCIAMENTO DE ACESSO, CONTROLE DE MUDANÇAS OPERACIONAIS) E CAPACITAÇÃO DOS ENVOLVIDOS (PROGRAMA DE CONSCIENTIZAÇÃO).	TI	TI	Imediato	1m	Internos	-
	2	RECOMENDAÇÕES DE SEGURANÇA - IMPLANTAR CONTROLES RECOMENDADOS NO ANEXO 9 – VULNERABILIDADE.	TI	TI	Imediato	1m	Internos	-
	3	GERENCIAMENTO DA CAPACIDADE – ESTUDO DE VIABILIDADE CONTEMPLANDO A SUBSTITUIÇÃO DOS SERVIDORES POR AMBIENTE VIRTUALIZADO COM ALTA DISPONIBILIDADE E DOCUMENTADO DENTRO DOS PADRÕES DE AQUISIÇÃO DEFINIDOS NA IN 04.	TI	TI	Imediato	1m	Internos	-



	4	GERENCIAMENTO DA CONTINUIDADE – ESTUDO DE VIABILIDADE DE SOLUÇÃO DE BACKUP QUE GARANTA A CONTINUIDADE DO NEGÓCIO E A EXECUÇÃO DA POLÍTICA DE BACKUP.	TI	TI	Imediato	1m	Internos	-
--	---	---	----	----	----------	----	----------	---

1ª ONDA	Nº	RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	5	REAVALIAR ESTRATEGIA – PARA RENOVAÇÃO DO PARQUE DE EQUIPAMENTOS CONTEMPLANDO O PADRÃO DE SOFTWARE E HARDWARE ESTABELECIDO	TI	TI	Em execução	1m	Interno	-
	6	ESTUDO PARA ADOÇÃO DE GERENCIADOR DE MAILING – AVALIAÇÃO DE SOLUÇÃO E ESTUDO DE IMPACTO NA REDE DE DADOS PARA ENVIO DE MALA DIRETA - DAED.	TI	TI	Out/11	1m	Interno	-
	7	PROJETO DE SOLUÇÃO CORPORATIVA DE WIRELESS SEGURA (EM EXECUÇÃO)	TI	TI	Em execução	1m	Interno	-
	8	DOCUMENTAR O PROJETO DE VIRTUALIZAÇÃO DENTRO DOS PADRÕES DE DOCUMENTAÇÃO PARA GERENCIAMENTO DE PROJETO (EM ESTUDO)	TI	TI	Em execução	1m	Interno	-

6.2. 2ª ONDA - AÇÕES DE MÉDIO PRAZO

2ª. Onda – duração 24 meses - ações que deverão ser deflagradas de Janeiro/2012 a Dezembro/2013, visando reforçar as condições para maior eficiência / eficácia de TI.

6.2.1. GOVERNANÇA DE TI

2ª ONDA	Nº	GOVERNANÇA DE TI	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	CAPACITAÇÃO DE TI – CONTINUAR A REALIZAÇÃO DE PALESTRAS E PROGRAMAS DE TREINAMENTO PARA TI E USUÁRIOS VISANDO MELHORAR: A COMUNICAÇÃO, A APRECIAÇÃO DE TI E A DIVULGAÇÃO D AS METAS INSTITUCIONAIS	TI	TI	Jan/12	3	Internos	-
	2	ESTABELECER PROGRAMA DE MELHORIA DOS PROCESSOS E PROCEDIMENTOS DE ADMINISTRAÇÃO DE DADOS CORPORATIVOS COM O OBJETIVO DE GERAÇÃO DA BASE DE CONHECIMENTO DA INSTITUIÇÃO.	TI	TI	Mar/12	1	Internos	-
	3	PDTI - REVER E ATUALIZAR O PDTI PARA O PERÍODO DE 2013-2014.	TI	TI	Out/12	1	Internos	-



6.2.2. GESTÃO DE PROJETOS E PROCESSOS

2ª ONDA	Nº	GESTÃO DE PROJETOS E PROCESSOS	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	GSTI - IMPLANTAR PROCESSOS COM FOCO EM GERENCIAMENTO DE INCIDENTES, PROBLEMAS E REQUISIÇÃO DE SERVIÇO.	TI	TI	Jan/12	2m	Externo	-
	2	GSTI - IMPLANTAR PROCESSOS DE GERENCIAMENTO DE MUDANÇA, CONFIGURAÇÃO E ATIVO DE SERVIÇO, LIBERAÇÃO, TESTE E VALIDAÇÃO	TI	TI	Mar/12	2m	Externo	-
	3	GSTI - IMPLANTAR PROCESSOS COM FOCO EM NIVEL DE SERVIÇO, CATALOGO DE SERVIÇOS, ACESSO, EVENTOS E SEGURANÇA.	TI	TI	Abr/12	2m	Externo	-
	4	GERÊNCIA DE PROJETOS - IMPLANTAR SISTEMÁTICA BÁSICA DE GERENCIAMENTO DE RISCOS DE TI PARA PROJETOS CRITICOS	TI	TI	Out/12	1m	Externo	-
	5	GSTI - IMPLANTAR PROCESSOS COM FOCO EM GERENCIAMENTO DE CAPACIDADE.	TI	TI	Jul/13	1m	Externo	-
	6	GSTI – IMPLANTAR PROCESSO COM FOCO EM GERENCIAMENTO DE FORNECEDORES.	TI	TI	Out/13	1m	Externo	-
	7	GSTI – PLANEJAMENTO E IMPLANTAÇÃO DO SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI) COM BASE NA NORMA NBR/ISO 27001.	TI	TI	Jan/12	7m	Externo	-



6.2.3. SERVIÇOS, SISTEMAS E APLICAÇÕES

2ª ONDA	Nº	SERVIÇOS, SISTEMAS E APLICAÇÕES	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	FERRAMENTA DE BUSCA DE DADOS NOS SISTEMAS SIGTEC, SCDP E FOLHA PARA PUBLICAÇÃO DE BOLETIM INTERNO	TI	TI	Jan/12	2m	Interno	-
	2	PALESTRAS DE CONSCIENTIZAÇÃO E ORIENTAÇÃO DE PROCEDIMENTOS DE SEGURANÇA E BACKUP.	TI	TI	Mar/12	1m	Interno	-



6.2.4. RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO

2ª ONDA	Nº	RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	AQUISIÇÃO DE INFRAESTRUTURA USUÁRIO - RENOVAÇÃO DE 25% DO PARQUE DE ESTAÇÕES DE TRABALHO A CADA ANO	TI	GETI	Jan/12	6m	Externo	-
	2	ESTUDO DE VIABILIDADE PARA CONTRATAÇÃO DE UM SERVIÇO DE INFRA-ESTRUTURA DE REDUNDÂNCIA E ALTA DISPONIBILIDADE EM UM SITE SEGURO PARA GARANTIR A EFICIENTE PRESTAÇÃO DE SERVIÇOS E EXECUÇÃO DAS APLICAÇÕES	TI	TI	Abr/12	3m	Interno	-
	3	DATA CENTER – NOVO DATA CENTER ATENDENDO AS NORMAS DE SEGURANÇA E P PROVER TODA A INFRAESTRUTURA E RECURSOS PARA SUPORTAR O AMBIENTE NECESSÁRIO QUE SE ENCONTRA DESCENTRALIZADO.	TI	TI	Jan/13	6m	Externo	-
	4	FERRAMENTA - IMPLANTAR FERRAMENTAS DE MONITORAMENTO DO AMBIENTE DE TI INTEGRADA COM A SOLUÇÃO DE GERENCIAMENTO DE SERVIÇOS DE TI.	TI	TI	Jan/13	3m	Interno	-
	5	FERRAMENTA - IMPLANTAR SOLUÇÃO DE GERENCIAMENTO DE SERVIÇOS DE TI EM CONFORMIDADE COM A VERSÃO 3 DA ITIL. (CENTRAL DE SERVIÇOS COM OS PROCESSOS DE REQ DE SERVIÇO, GER DE INCIDENTES E GER. PROBLEMAS	TI	TI	Out/12	3m	Externo	-
	6	FERRAMENTA - IMPLANTAR FERRAMENTA PARA GERENCIAMENTO DE ACESSO E IDENTIDADE	TI	TI	Jan/13	3m	Externo	-
	7	ANÁLISE DE VULNERABILIDADE – REALIZAR A ANALISE DE VULNERABILIDADE INTERNA E EXTERNA ANUALMENTE (SERVIDORES, ESTAÇÕES, SWITCHES, ROUTERS, FIREWALLS, CÓDIGO DE APLICAÇÕES	TI	TI	Jul/13	1m	Externo	-
	8	CERTIFICAÇÃO – PROJETO CERTIFICAÇÃO PARA ACESSOS EXTERNOS	TI	TI	Jan/12	1m	Externo	-
	9	POLITICA DE SEGURANÇA – AMPLIAR A POLITICA DE SEGURANÇA	TI	TI	Out/13	1m	Interno	-

	10	ESTUDO DE VIABILIDADE - MODERNIZAÇÃO DA REDE DE DADOS CORPORATIVA – ESTUDO DE VIABILIDADE PARA AUMENTO DE CAPACIDADE DA REDE DE DADOS CORPORATIVA	TI	TI	Out/13	1m	Interno	-	
	11	ESTUDO DE VIABILIDADE PARA AQUISIÇÃO DE FERRAMENTA DE RISCO	TI	TI	Jul/13	1m	Interno	-	
	12	FERRAMENTA – AMPLIAR SOLUÇÃO DE GERENCIAMENTO DE SERVIÇOS DE TI EM CONFORMIDADE COM A VERSÃO 3 DA ITIL. (PROCESSOS GER. DE MUDANÇA, CONFIGURAÇÃO E ATIVO DE SERVIÇO, LIBERAÇÃO, TESTE E VALIDAÇÃO)	TI	TI	Abr/13	6m	Externo	-	



6.3. 3ª ONDA – 24 MESES

3ª. Onda – duração 24 meses - ações de longo prazo que deverão ser deflagradas de Janeiro/2014 a Dezembro/2015, visando melhorar nível de serviços aos clientes internos e externos e da segurança.

6.3.1. GOVERNANÇA DE TI

3ª ONDA	Nº	GOVERNANÇA DE TI	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	DIAGNÓSTICO – AVALIAR OS PROCESSOS DE GERENCIAMENTO DE SERVIÇOS DE TI COM BASE NA NORMA NBR ISO/IEC 20000-1 E 27001.	TI	TI	Jan/15	3m	Externo	-
	2	AUDITORIA – REALIZAR AUDITORIA PARA CERTIFICAÇÃO DO SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO - NBR ISO/IEC 27001.	TI	TI	Mar/15	3m	Externo	-
	3	PDTI - ELABORAÇÃO DO NOVO PDTI 2016-2020.	TI	TI	Jun/15	3m	Externo	-



6.3.2. GESTÃO DE PROJETOS E PROCESSOS

3ª ONDA	Nº	GESTÃO DE PROJETOS E PROCESSOS	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	GSTI - IMPLANTAR PROCESSO COM FOCO EM GERENCIAMENTO DE CONTINUIDADE DE SERVIÇOS DE TI	TI	TI	Jan/14	1m	Externo	-
	2	APERFEIÇOAR O FLUXO DE GESTÃO DAS DEMANDAS e da CAPACIDADE ATENDIMENTO E O FLUXO DE GESTÃO DE RECURSOS, INFRAESTRUTURA E AQUISIÇÕES	TI	TI	Mar/14	1m	Interno	-
	3	GESTÃO DE PROCESSOS - IMPLANTAR METODOLOGIA DE GESTÃO DE PROCESSOS DE NEGÓCIO	TI	TI	Abr/14	1m	Externo	-
	4	GERÊNCIA DE PROJETOS – AMPLIAR METODOLOGIA DE GESTÃO DE PROJETOS.	TI	TI	Jun/14	1m	Interno	-
	5	METODOLOGIA E PADRÕES TÉCNICOS DE DESENVOLVIMENTO DE SISTEMAS - AMPLIAR METODOLOGIA DE DESENVOLVIMENTO DE SISTEMAS, ESTABELECENDO OS PROCEDIMENTOS, MÉTODOS E PADRÕES DE DESENVOLVIMENTO E SELECCIONAR, INSTALAR E TREINAR OS DESENVOLVEDORES NAS FERRAMENTAS ADOTADAS (MODELAGEM, DESENVOLVIMENTO, LIBERAÇÃO E DISTRIBUIÇÃO E TESTES)	TI	TI	Jul/14	2m	Externo	-



6.3.3. SERVIÇOS, SISTEMAS E APLICAÇÕES

3ª ONDA	Nº	SERVIÇOS, SISTEMAS E APLICAÇÕES	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	DEFINIR ESTUDO E ELABORAR PROJETO - MODELO DE DADOS PARA REPOSITORIO DE INFORMAÇÕES DE PESQUISA E ADOÇÃO DE FERRAMENTA.	TI	TI	Jan/14	6m	Interno	-
	2	DEFINIR MODELO DE ARQUITETURA DE DADOS E APERFEIÇOAR O FLUXO DE GESTÃO DA INFORMAÇÃO VISANDO ORGANIZAR DADOS, DISPONIBILIZAR INFORMAÇÕES E DESENVOLVER O CONHECIMENTO RESULTANTE DOS PROCESSOS.	TI	TI	Jan/14	6m	Interno	-

**6.3.4. RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO**

3ª Onda	Nº	RECURSOS TECNOLÓGICOS E GESTÃO DA SEGURANÇA DA INFORMAÇÃO	RESPONS. PROPOR	RESPONS. APROVAR	DATA INÍCIO	DURAÇÃO	RECURSOS	CUSTO (R\$ mil)
		AÇÕES						
	1	AQUISIÇÃO DE INFRAESTRUTURA USUÁRIO - RENOVAÇÃO DE 25% DO PARQUE DE ESTAÇÕES DE TRABALHO A CADA ANO	TI	TI	Mar/14	3m	Interno	-
	2	ANÁLISE DE VULNERABILIDADE – REALIZAR A ANALISE DE VULNERABILIDADE INTERNA E EXTERNA ANUALMENTE (SERVIDORES, ESTAÇÕES, SWITCHES, ROUTERS, FIREWALLS, CÓDIGO DE APLICAÇÕES)	TI	TI	Jun/14	1m	Interno	-
	3	POLITICA DE SEGURANÇA – AMPLIAR A POLITICA DE SEGURANÇA	TI	TI	Out/14	1m	Interno	-