COGEP
BOLETIM
DE PESSOAL E SERVIÇO

Ministério do Turismo
GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

Sumário

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

1. Atos da Secretaria-Executiva

1.1. Portarias da Comissão Permanente de Correição

Portaria nº 35, de 19 de dezembro de 2013

O COORDENADOR DA COMISSÃO PERMANENTE DE CORREIÇÃO DO MINISTÉRIO DO TURISMO, no uso das atribuições que lhe confere o inciso VII do art. 7º da Portaria/GM nº 284, de 28 de agosto de 2012, do Ministério do Turismo, em conformidade com os artigos 5º e 11 da Portaria-CGU nº 335, de 30 de maio de 2006 e, com o artigo 143 da Lei nº 8.112, de 11 de dezembro de 1990,

R E S O L V E:

Art. 1º - Prorrogar por mais 30 (trinta) dias, o prazo estabelecido pela Portaria da Comissão Permanente de Correição/SE-MTur nº 30, de 21 de novembro de 2013, para conclusão dos trabalhos da Comissão de Sindicância Investigativa, ante as razões apresentadas no Memorando nº 002/CS/MTur, de 19 de dezembro de 2013, a contar de 23 de dezembro de 2013.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação.

VANDIR CHALEGRA CASSIANO

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

1. Atos da Secretaria-Executiva

1.1. Portarias da Comissão Permanente de Correição

Portaria nº 36, de 19 de dezembro de 2013

O COORDENADOR DA COMISSÃO PERMANENTE DE CORREIÇÃO DO MINISTÉRIO DO TURISMO, no uso das atribuições que lhe confere o inciso VII do art. 7º da Portaria/GM nº 284, de 28 de agosto de 2012, do Ministério do Turismo, em conformidade com os artigos 5º e 11 da Portaria-CGU nº 335, de 30 de maio de 2006 e, com o artigo 143 da Lei nº 8.112, de 11 de dezembro de 1990,

R E S O L V E:

Art. 1º - Prorrogar por mais 30 (trinta) dias, o prazo estabelecido pela Portaria da Comissão Permanente de Correição/SE-MTur nº 29, de 21 de novembro de 2013, para conclusão dos trabalhos da Comissão de Sindicância Investigativa, ante as razões apresentadas no Memorando nº 002/CS/MTur, de 19 de dezembro de 2013, a contar de 23 de dezembro de 2013.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação.

VANDIR CHALEGRA CASSIANO

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

1. Atos da Secretaria-Executiva

1.1. Portarias da Comissão Permanente de Correição

Portaria nº 37, de 19 de dezembro de 2013

O COORDENADOR DA COMISSÃO PERMANENTE DE CORREIÇÃO DO MINISTÉRIO DO TURISMO, no uso das atribuições que lhe confere o inciso VII do art. 7º da Portaria/GM nº 284, de 28 de agosto de 2012, do Ministério do Turismo, em conformidade com os artigos 5º e 11 da Portaria-CGU nº 335, de 30 de maio de 2006 e, com o artigo 143 da Lei nº 8.112, de 11 de dezembro de 1990,

R E S O L V E:

Art. 1º - Prorrogar por mais 30 (trinta) dias, o prazo estabelecido pela Portaria da Comissão Permanente de Correição/SE-MTur nº 28, de 21 de novembro de 2013, para conclusão dos trabalhos da Comissão de Sindicância Investigativa, ante as razões apresentadas no Memorando nº 002/CS/MTur, de 19 de dezembro de 2013, a contar de 23 de dezembro de 2013.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação.

VANDIR CHALEGRA CASSIANO

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

1. Atos da Secretaria-Executiva

1.1. Portarias da Comissão Permanente de Correição

Portaria nº 38, de 19 de dezembro de 2013

O COORDENADOR DA COMISSÃO PERMANENTE DE CORREIÇÃO DO MINISTÉRIO DO TURISMO, no uso das atribuições que lhe confere o inciso VII do art. 7º da Portaria/GM nº 284, de 28 de agosto de 2012, do Ministério do Turismo, em conformidade com os artigos 5º e 11 da Portaria-CGU nº 335, de 30 de maio de 2006 e, com o artigo 143 da Lei nº 8.112, de 11 de dezembro de 1990,

R E S O L V E:

Art. 1º - Prorrogar por mais 30 (trinta) dias, o prazo estabelecido pela Portaria da Comissão Permanente de Correição/SE-MTur nº 34, de 22 de novembro de 2013, para conclusão dos trabalhos da Comissão de Sindicância Investigativa, ante as razões apresentadas no Memorando nº 003/CSI Portaria mº 34/CPCor/SE/MTur, de 19 de dezembro de 2013, a contar de 23 de dezembro de 2013.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação.

VANDIR CHALEGRA CASSIANO

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

1. Atos da Secretaria-Executiva

1.1. Portarias da Comissão Permanente de Correição

Portaria nº 39, de 19 de dezembro de 2013

O COORDENADOR DA COMISSÃO PERMANENTE DE CORREIÇÃO DO MINISTÉRIO DO TURISMO, no uso das atribuições que lhe confere o inciso VII do art. 7º da Portaria/GM nº 284, de 28 de agosto de 2012, do Ministério do Turismo, em conformidade com os artigos 5º e 11 da Portaria-CGU nº 335, de 30 de maio de 2006 e, com o artigo 143 da Lei nº 8.112, de 11 de dezembro de 1990,

R E S O L V E:

Art. 1º - Prorrogar por mais 30 (trinta) dias, o prazo estabelecido pela Portaria da Comissão Permanente de Correição/SE-MTur nº 33, de 22 de novembro de 2013, para conclusão dos trabalhos da Comissão de Sindicância Investigativa, ante as razões apresentadas no Memorando nº 003/CSI Portaria mº 33/CPCor/SE/MTur, de 19 de dezembro de 2013, a contar de 23 de dezembro de 2013.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação.

VANDIR CHALEGRA CASSIANO

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

1. Atos da Secretaria-Executiva

1.1. Portarias da Comissão Permanente de Correição

Portaria nº 40, de 19 de dezembro de 2013

O COORDENADOR DA COMISSÃO PERMANENTE DE CORREIÇÃO DO MINISTÉRIO DO TURISMO, no uso das atribuições que lhe confere o inciso VII do art. 7º da Portaria/GM nº 284, de 28 de agosto de 2012, do Ministério do Turismo, em conformidade com os artigos 5º e 11 da Portaria-CGU nº 335, de 30 de maio de 2006 e, com o artigo 143 da Lei nº 8.112, de 11 de dezembro de 1990,

R E S O L V E:

Art. 1º - Prorrogar por mais 30 (trinta) dias, o prazo estabelecido pela Portaria da Comissão Permanente de Correição/SE-MTur nº 32, de 22 de novembro de 2013, para conclusão dos trabalhos da Comissão de Sindicância Investigativa, ante as razões apresentadas no Memorando nº 003/CSI Portaria mº 32/CPCor/SE/MTur, de 09 de dezembro de 2013, a contar de 23 de dezembro de 2013.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação.

VANDIR CHALEGRA CASSIANO

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

2. Atos da Secretaria-Executiva

2.1. Resoluções da Secretaria-Executiva

Resolução nº 4, de 27 de novembro de 2013

Aprova o Plano Diretor de Segurança da Informação e Comunicações – PDSIC do Ministério do Turismo.

O COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO MINISTÉRIO DO TURISMO, instituído pela Portaria MTur nº 344, de 26 de outubro 2012, no uso das atribuições que lhe confere o inciso V do art. 4º,

R E S O L V E:

Art. 1º Fica aprovado, na forma do Anexo, o Plano Diretor de Segurança da Informação e Comunicações – PDSIC, que fornece as diretrizes de Segurança da Informação aplicáveis às informações custodiadas ou de propriedade do Ministério do Turismo disponibilizadas no ambiente de Tecnologia da Informação, visando estabelecer as ações e medidas que deverão ser realizadas para implementar processos recorrentes da Gestão de Segurança da Informação e Comunicações – GSIC.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

SERGIO BRAUNE SOLON DE PONTES

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

ANEXO

MTur
Segurança da Informação e Comunicações

MINISTÉRIO DO TURISMO

Plano Diretor de Segurança da Informação e Comunicações - PDSIC

2013-2015

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

Ministério do Turismo

Gastão Dias Vieira
Ministro de Estado

Comitê de Segurança da Informação e Comunicações - CSIC

Sérgio Braune Solon de Pontes
Secretário-Executivo
Presidente do Comitê de Segurança da Informação e Comunicações

Vinícius Rene Lummertz Silva
Secretário Nacional de Políticas de Turismo

Fábio Rios Mota
Secretário Nacional de Programas de Desenvolvimento do Turismo

Mauro Borges Ribeiro Formiga
Chefe de Gabinete do Ministro de Estado

José Raimundo Machado dos Santos
Ouvidor

Manoelina Pereira Medrado
Consultora Jurídica

Luis Henrique Fanan
Diretor de Gestão Estratégica

Rubens Portugal Bacellar
Diretor de Gestão Interna

Paulo Roberto de Souza Lemos
Coordenador-Geral de Tecnologia da Informação

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

Núcleo de SIC

Sumaid Andrade de Albuquerque
Gerente do Projeto

Marcelo Araújo Resende

Marcelo Mafra Leal

Marcelo Silva Hemerly

Maria Aparecida Gomes

O Núcleo de Segurança da Informação e Comunicações é gerenciado pelo Gestor de Segurança da Informação e Comunicações, designado para implantar o Programa de Segurança da Informação e Comunicações do Ministério do Turismo e elaborar o Plano Diretor de Segurança da Informação e Comunicações - PDSIC conforme Termo de Abertura do Projeto EGPTI_025 do Escritório de Gerenciamento de Projetos da TI (EGP-TI).

A aprovação do PDSIC é realizada pelo Comitê de SIC do Ministério do Turismo instituído pela Portaria Nº 344, de 26 de junho de 2012.

Brasília – DF
2013

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

1 Contexto Geral

1.1 Apresentação

Este documento intitulado Plano Diretor de Segurança da Informação e Comunicações - PDSIC 2013/2015, fornece as diretrizes de Segurança da Informação aplicáveis às informações custodiadas ou de propriedade do Ministério do Turismo – MTur disponibilizadas no ambiente de Tecnologia da Informação, visando estabelecer as ações e medidas que o MTur deve realizar para implementar processos recorrentes da Gestão de Segurança da Informação e Comunicações - GSIC.

A implantação de um sistema de GSIC é um dos objetivos estratégicos de TI no MTur, tendo como finalidade garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações dos ativos que agregam valor, sejam eles estratégicos, táticos ou operacionais, internos ou externos.

Para o desenvolvimento desse PDSIC, foram levantadas informações a partir do Inventário e Mapeamento dos Ativos de Informação da Coordenação-Geral de Tecnologia da Informação, bem como a Análise de Riscos desses ativos e as leis, normas e melhores práticas de Segurança da Informação e Comunicações.

A instituição do Comitê de Segurança da Informação e Comunicações – CSIC do Ministério do Turismo concretiza-se como um marco fundamental na busca de efetivamente implementar ações de Segurança da Informação e principalmente na busca da organização dos processos de segurança que irão suportar o órgão no conhecimento, definição, implementação, monitoração e manutenção dos níveis adequados de Segurança da Informação e Comunicações.

O planejamento de elaboração do PDSIC teve como escopo 03 (três) etapas de trabalho, na qual cada grupo tem um propósito específico, conforme abaixo:

- Definições Preliminares – Realização de análise do MTur, sendo consideradas as características do órgão e as restrições a que estão sujeitas, objetivando definir o escopo e a metodologia de trabalho;
- Inventário e Mapeamento dos Ativos de Informação – Levantamento de um conjunto de informações básicas dos ativos de informação da Coordenação-Geral de Tecnologia da Informação;
- Gestão de Riscos – Processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibra-los com os custos operacionais e financeiros envolvidos.

1.2 Introdução

O Governo Federal tem demonstrado, por meio de seus órgãos de controle, que a Segurança da Informação é um objetivo claro para a melhoria dos processos de negócio de toda sua estrutura.

Em 2008 o Tribunal de Contas da União realizou o "*Levantamento acerca da Governança de Tecnologia da Informação*" na Administração Pública Federal. O levantamento relata por meio do ACÓRDÃO Nº 1603/2008 – TCU – PLENÁRIO, que "*o aspecto em que a situação da governança de TI está mais crítica é no que diz respeito ao tratamento da segurança da informação. Conclui-se que essa é uma área em que o TCU pode, e deve, atuar como indutor do processo de aperfeiçoamento da governança de TI. O Tribunal já acertou, inclusive, ao editar, em 2003 e 2007, a "Cartilha de Segurança da Informação" para servir como orientação sobre o tema. Outra maneira de induzir a melhoria no tratamento da segurança é a realização de auditorias de TI com foco em segurança da informação, que poderão fornecer subsídios valiosos para os gestores sobre os principais controles que devem ser implementados visando garantir a confiabilidade, a integridade e a disponibilidade das informações tratadas pelos órgãos/entidades da Administração Pública Federal*".

Ainda, segundo o Acórdão 2.308/2010 – TCU a "*segurança da informação continua a chamar atenção pelos altos índices de não-conformidade, sugerindo que, de forma geral, as organizações públicas, além de não tratarem os riscos aos quais estão expostas, os desconhecem".*

Conforme recomendações da Instrução Normativa 01 publicada pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR e suas Normas Complementares de SIC; e ainda o Levantamento acerca da Governança de Tecnologia da Informação, publicada pelo TCU, o MTur deverá estar aderente as melhores práticas de Segurança da Informação e Comunicações com o objetivo de promover a cultura de SIC no Órgão. Além da busca por conformidade com as melhores práticas de mercado, é necessário que o Ministério do Turismo atenda as diretrizes da Política de Segurança da Informação e Comunicações - POSIC, publicada no D.O.U - Portaria Nº 108, de 22 de maio de 2013.

Ressalta-se que este documento é instrumento para nortear as atividades relacionadas à Segurança da Informação e Comunicações e oferece ao Comitê de Segurança da Informação e Comunicações – CSIC subsídios para execução de projetos de SIC, a fim de definir os aspectos de priorização, esforço, custeio e recursos necessários para nortear a execução de projetos ligados à Segurança da Informação e Comunicações no âmbito do Ministério do Turismo.

1.3 Objetivo

O Plano Diretor de Segurança da Informação e Comunicações – PDSIC visa organizar e planejar as ações de SIC, no âmbito do Ministério do Turismo, baseando-se nas recomendações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR e melhores práticas de Segurança da Informação.

1.4 Abrangência

O PDSIC abrange os processos, as pessoas, as tecnologias e os ambientes vinculados a Coordenação-Geral de Tecnologia da Informação do Ministério do Turismo de modo temporário ou permanente.

1.5 Vigência

O PDSIC terá a vigência de três anos a contar da data de sua publicação, com revisões e validações anuais. A cada 03 (três) anos, deve-se elaborar novo PDSIC. Este será aprovado e implementado com o objetivo de garantir o ciclo e a manutenção do Sistema de Gestão de Segurança da Informação – SGSI no âmbito do MTur.

1.6 Conceitos e Definições

CONCEITOS	DESCRIÇÃO
Acesso	Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade [NC07/IN01/DSIC/GSIPR, 2010, p. 2].
Ameaça	Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização [NC04/IN01/DSIC/GSIPR, 2013, p. 2].
Ativo	Tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal.
Ativos de Informação	Meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso [NC04/IN01/DSIC/GSIPR, 2013, p. 3].
Autenticidade	Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2].
Capacitação em SIC	Saber o que é Segurança da Informação e Comunicações aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na Organização como gestor de SIC. [DSIC/GSIPR].

CONCEITOS	DESCRIÇÃO
Capacitação	Visa à aquisição de conhecimentos, capacidades, atitudes e formas de comportamento exigido para o exercício das funções.
Classificação da Informação	Identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.
Comitê de Segurança da Informação e Comunicações - CSIC	Instância estratégica responsável por tratar e deliberar a respeito de temas na área de Segurança da Informação e Comunicações [NC03/IN01/DSIC/GSIPR, 2009, p. 2].
Confidencialidade	Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado [IN01/DSIC/GSIPR, 2008, p. 2].
Conscientização em SIC	Saber o que é Segurança da Informação e Comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema. [DSIC/GSIPR].
Continuidade de Negócios	Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido [NC06/IN01/DSIC/GSIPR, 2009, p. 3].
Controle de Acesso	Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso [NC07/DSIC/GSIPR, 2010, p. 3].
CTIR.GOV	Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República [NC05/IN01/DSIC/GSIPR,2009 p. 3].
Custodiante	Responsável por armazenar e preservar as informações que não lhe pertencem, refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação e Comunicações comunicadas pelos proprietários dos ativos de informação [NC10/DSIC/GSIPR, 2012, p. 2].
Disponibilidade	Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2].
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR	Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores [NC05/IN01/DSIC/GSIPR,2009 p. 3].
Estrutura de GSIC	Grupo responsável pela gestão e execução da Segurança da Informação e Comunicações – SIC.
Evento	Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma

CONCEITOS	DESCRIÇÃO
	situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004].
Gestão de Riscos de Segurança da Informação e Comunicações	Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos [NC04/IN01/DSIC/GSIPR, 2013, p.3].
Gestão de Segurança da Informação e Comunicações	Ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações [IN01/DSIC/GSIPR, 2008, p. 2].
Gestor de Segurança da Informação e Comunicações	Servidor responsável pelas ações de Segurança da Informação e Comunicações no âmbito do Ministério do Turismo [NC03/IN01/DSIC/GSIPR, 2009, p. 2].
Incidente de Segurança	É qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores [NC05/IN01/DSIC/GSIPR, 2009, p. 3].
Informação Estratégica	Toda a informação corporativa relativa à administração, planejamento, estrutura, gestão, relações internas e externas, novos produtos e tecnologias, serviços e contratos.
Integridade	Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental [IN01/DSIC/GSIPR, 2008, p. 2].
Nível de Segurança Adequado	Métricas de seguranças estabelecidas para uma rede ou sistema, depois de identificado o potencial de ameaça.
Política de Segurança da Informação e Comunicações - POSIC	Documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficiente à implementação da Segurança da Informação e Comunicações [NC03/IN01/DSIC/GSIPR, 2009, p. 2].
Proprietário da Informação	Pessoa ou setor que produz a informação, capaz de estimar em que nível de criticidade cada uma se enquadra.
Quebra de Segurança	Ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e das Comunicações [IN01/DSIC/GSIPR, 2008, p. 2].
Recursos Criptográficos	Sistemas, programas, processos e equipamentos isolados ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração.
Riscos de Segurança da Informação e Comunicações	Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização [NC04/IN01/DSIC/GSIPR, 2013, p.3].
Segurança da Informação e Comunicações	Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações [IN01/DSIC/GSIPR, 2008, p. 2].
Segurança de Operações e Comunicações	Definição de parâmetros responsáveis pela manutenção do funcionamento de serviços, sistemas e da infraestrutura que os suporta.
Sensibilização em SIC	Ações que visão identificar, recomendar, criar e implementar programas de conscientização, a fim de proporcionar melhorias e mudanças na atitude e na

CONCEITOS	DESCRIÇÃO
	educação organizacional quanto à importância da Segurança da Informação em todos os níveis do órgão.
Sistemas Estruturantes	Conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente.
Terceiro	Quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao MTur, envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.
Usuário	Servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade [NC07/DSIC/GSIPR, 2010, p. 3].
Vulnerabilidade	Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de Segurança da Informação NC04/IN01/DSIC/GSIPR, 2013, p.4].

Tabela 1 – Conceitos e Definições

1.7 Alinhamento Estratégico

O MTur tempo por missão: "*Desenvolver o turismo sustentável brasileiro como uma atividade economicamente competitiva, com papel relevante na geração de renda, emprego e divisas, na inclusão social, na redução de desigualdades regionais e na preservação do meio ambiente*".

Para cumprir sua missão, o Ministério tem como visão "*Posicionar o Brasil como uma das três maiores economias turísticas do mundo até 2022"*.

Derivados dessa missão e visão, com a implementação de um Sistema de Gestão de Segurança da Informação e Comunicações no MTur, os seguintes objetivos do planejamento estratégico serão favorecidos:

- Aperfeiçoar o controle interno, a gestão de riscos e a segurança institucional;
- Simplificar e uniformizar normas, processos e procedimentos;
- Prover soluções integradas de tecnologia e comunicações, segura e de alto desempenho.

Ações que garantam a disponibilidade de informações, gestão de riscos e classificação das informações corporativas trazem benefícios que suplantam o âmbito administrativo do MTur, tornando-se um elemento auxiliar no alcance dos objetivos estratégicos definidos ao turismo brasileiro. Para tanto, este PDSIC deverá ser reconhecido como parte integrante do planejamento estratégico do MTur, atendendo as áreas de negócio, e não se limitando a Tecnologia da Informação.

1.8 Escopo

O PDSIC teve como escopo de trabalho a realização do levantamento da situação atual do Órgão e seu diagnóstico em relação à aderência da Segurança da Informação com o foco inicial na área de Tecnologia da Informação.

Foram abrangidas as diretrizes gerais, definidas na NC03 do GSI, em seu item 5.3.5:

a) Tratamento da Informação;
b) Tratamento de Incidentes de Rede;
c) Gestão de Risco;
d) Controles de Acesso;
e) Uso de e-mail; e
f) Acesso a Internet.

1.9 Metodologia Aplicada

A elaboração do PDSIC baseou-se na metodologia de Gestão de Segurança da Informação e Comunicações denominado ciclo "PDCA" (*Plan-Do-Check-Act*), referenciado pela Norma Complementar nº 02/IN01/DSIC/GSIPR de 13 de agosto de 2008.

Por ser um processo de melhoria contínua, a escolha desta metodologia levaram em consideração três critérios:

a) Simplicidade do modelo;
b) Compatibilidade com a cultura de Gestão de Segurança da Informação em uso nas organizações públicas e privadas brasileiras;

c) Coerência com as práticas de qualidade e gestão adotadas em órgãos públicos brasileiros.

A Figura 1 demonstra a metodologia do Ciclo PDCA:

Figura 1 - Ciclo PDCA

O processo de construção deste Plano foi realizado com base na metodologia de gerenciamento de projetos adotada no Ministério do Turismo, definida pelo Escritório de Gerenciamento de Projetos da CGTI.

As atividades realizadas compreenderam as fases de:

Preparação – com a definição da equipe de elaboração, aprovação do plano de projeto, levantamento e análise de documentos de referência, estratégias da organização e princípios e diretrizes norteadoras do trabalho.

Diagnóstico – definição do escopo de trabalho e a metodologia a ser adotada, inventário e mapeamento dos ativos de informação da Coordenação-Geral de Tecnologia da Informação com relação à coleta de informações gerais, detalhamento dos ativos e identificação dos responsáveis, e a análise de riscos desses ativos. Esse diagnóstico constitui uma etapa importante para a definição das necessidades de Segurança do Órgão.

Redação da Minuta do PDSIC – consolidação das necessidades de SIC levantadas, alinhamento das necessidades com as estratégias da organização e explanação do plano de ações desejado para a Segurança da Informação do MTur. Foram consideradas as informações obtidas no Inventário e Mapeamento dos Ativos

de Informação da Coordenação-Geral de Tecnologia da Informação e na Análise de Riscos realizada. Assim como, as recomendações das Normas de SIC do Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Encaminhamentos – encaminhamento da Minuta do PDSIC para o Gestor de SIC e para o Comitê de SIC para deliberações estratégicas do Órgão.

As atividades supramencionadas objetivam diagnosticar os riscos potenciais do Órgão, identificando ameaças, vulnerabilidades, riscos e impactos potenciais ao negócio do Ministério.

As informações coletadas ajudaram a definir as principais necessidades de segurança do ambiente de TI do MTur e os pontos a serem contemplados nesse PDSIC. A priorização da execução de projetos e ações de segurança ao longo dos próximos três anos foi identificada observando os índices de riscos gerados na análise de riscos.

1.10 Princípios e Diretrizes

Na Tabela 2 estão listados os princípios e diretrizes que nortearam o desenvolvimento desse plano, com suas respectivas origens:

PD1	Aperfeiçoar o controle interno, a gestão de riscos e a segurança institucional.	Planejamento de Gestão Estratégica do Ministério do Turismo 2012-2015.
PD2	Simplificar e uniformizar normas, processos e procedimentos.	Planejamento de Gestão Estratégica do Ministério do Turismo 2012-2015.
PD3	Prover soluções integradas de tecnologia e comunicação, seguras e de alto desempenho.	Planejamento de Gestão Estratégica do Ministério do Turismo 2012-2015.
PD4	Aderência às decisões e normas do Comitê de SIC do MTur.	Portaria Nº 344, de 26 de outubro de 2012. Portaria Nº 108, de 22 de maio de 2013. Resolução Nº 03, de 29 de maio de 2013.

Tabela 2 – Princípios e Diretrizes

1.11 Estrutura Organizacional da Unidade de TI do MTur

A área de Tecnologia da Informação deve ser entendida como o elemento organizacional responsável pela estruturação, utilização e disponibilização do ferramental tecnológico de suporte aos programas, atividades e ações de todas as unidades do Ministério do Turismo. No MTur, as atividades de TI são gerenciadas de forma centralizada pela Coordenação Geral de Tecnologia da Informação (CGTI).

A CGTI é ligada organizacionalmente à Diretoria de Gestão Interna (DGI), que por sua vez é subordinada à Secretaria-Executiva do MTur. O organograma da Figura 2 apresenta a organização do MTur até o nível de Diretorias/Departamentos, salientando a localização da CGTI na estrutura do Órgão.

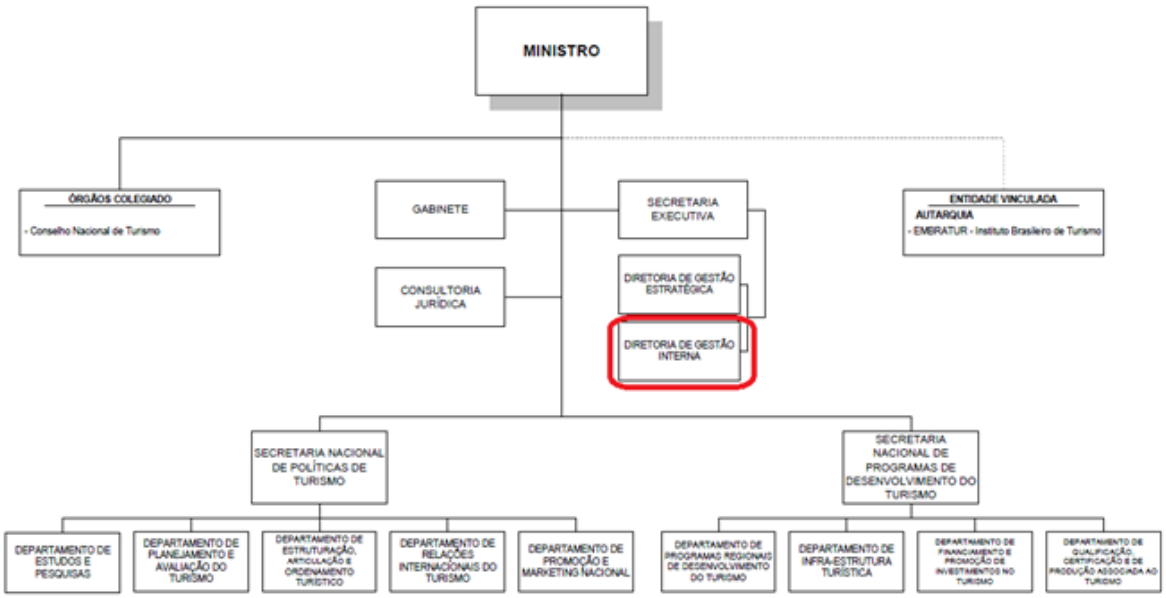

Figura 2 - Organograma do Ministério do Turismo - Destaque na DGI

A CGTI foi concebida para assegurar ao MTur o suporte de informação sistematizado, adequado, dinâmico, confiável e eficaz, além de facilitar aos usuários o acesso a informações disponíveis. Seus esforços estão atualmente concentrados em alinhar-se ao negócio do MTur, agregando-lhe valor.

A CGTI tem se organizado segundo conjuntos de atividades de natureza semelhante, tanto na utilização de seus recursos internos, quanto para a gestão dos contratos com fornecedores, conforme ilustrado e descrito na Figura 3. Tal estrutura não está formalizada. Ressalta-se, entretanto, que, com a condução de projeto de Mapeamento de Competências na CGTI, uma nova estrutura funcional será proposta para essa Coordenação, de forma que possa melhor se adequar à estratégia de TI do Órgão.

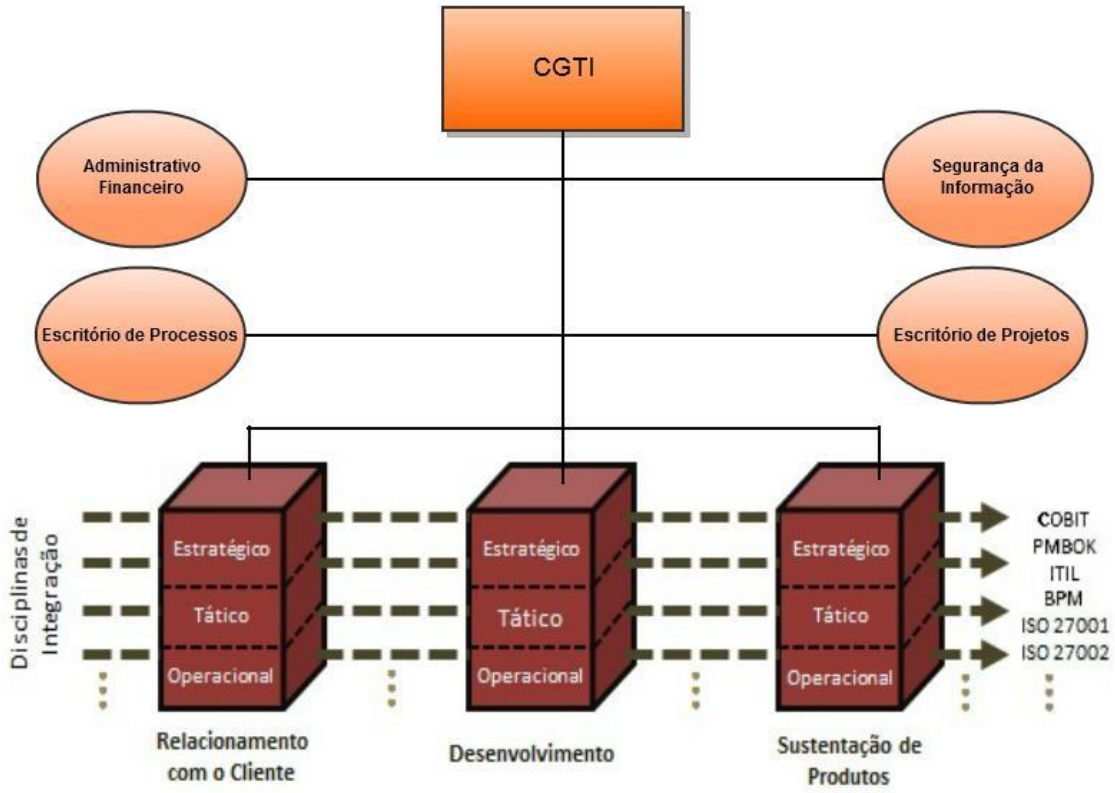

Figura 3 - Organização da CGTI/MTur

A Coordenação-Geral de TI é apoiada pelo Escritório de Planejamento e Gestão de TI, composto pelas áreas Administrativo-Financeiro, Segurança da Informação, Escritório de Processos, Escritório de Projetos, Relacionamento com o Cliente, Desenvolvimento e Sustentação de Produtos e Serviços (subdividida em Infraestrutura, Manutenção de Sistemas e Suporte Técnico). Dentre suas responsabilidades está o planejamento e a gestão dos processos de TI relacionados. Suas tarefas permeiam os níveis estratégico, tático e operacional, e utilizam disciplinas de integração referenciadas pelas boas práticas de governança e gestão de TI.

O Coordenador-Geral de TI concentra as atividades de interlocução com a DGI e com as outras áreas finalísticas e de apoio do MTur; decisões gerenciais e estratégicas de TI, entre outras. De acordo com esses conjuntos de atividades, essas áreas são:

a) Administrativo-Financeiro: responsável pela gestão dos contratos, gestão orçamentária, gestão de pessoal, relacionamento institucional, auditorias e conformidade legal;

b) Segurança da Informação e Comunicações: responsável pela gestão do sistema de segurança da informação e comunicações, pela garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações;

c) Escritório de Processos de TI: responsável pelo mapeamento e melhoria dos processos de TI e tem o objetivo de implantar a gestão por processos, por meio do apoio técnico e metodológico no mapeamento, análise e melhoria dos processos organizacionais, vislumbrando a excelência na prestação de serviços e no alcance dos objetivos de negócio da instituição;

d) Escritório de Projetos de TI: responsável por apoiar o desenvolvimento das práticas de gerenciamento dos projetos na CGTI. Ele fornece apoio às equipes de projeto e informações à coordenação de TI e demais partes interessadas nos projetos;

e) Relacionamento com o Cliente: responsável pelas atividades relacionadas à interface da CGTI com as demais áreas do Ministério, gestão do atendimento das demandas, responsável pelas análises de requisitos de novos sistemas e análises do ambiente de negócio;

f) Desenvolvimento: responsável pelo planejamento e gestão do desenvolvimento de sistemas e pela definição da metodologia de desenvolvimento; programação, testes e implantação de sistemas informatizados. Monitora o processo de desenvolvimento e certifica a aderência aos padrões estabelecidos;

g) Sustentação de Produtos e Serviços: responsável pelas atividades que garantem a entrega de produtos e serviços de TI de acordo com os níveis exigidos. Subdivide-se em três áreas:

g.1) Infraestrutura: responsável pelas atividades relativas à sustentação do ambiente tecnológico propriamente dito - computadores servidores, ativos de rede, links de comunicação, equipamentos de backup, serviços de armazenamento e etc;

g.2) Manutenção de Sistemas: responsável pelas atividades relacionadas à realização de correções, adaptações e melhorias evolutivas dos sistemas em operação;

g.3) Suporte Técnico: responsável pelas atividades relativas ao cotidiano dos usuários, manutenção e movimentação de computadores, impressoras, suporte à utilização de software básico e etc.

Essas atividades são desempenhadas em 3 diferentes níveis de responsabilidade:

- Estratégico: responsável por definir a necessidade e o direcionamento das políticas de TI. Composto pelo Coordenador da CGTI e pela alta Administração do Ministério.
- Tático: responsável pela elaboração das políticas de TI, de acordo com as diretrizes do nível estratégico. Composto exclusivamente por servidores públicos.
- Operacional: responsável pela execução dos serviços da CGTI, em conformidade com as políticas de TI estabelecidas. Composto preferencialmente por funcionários terceirizados, podendo também haver servidores públicos.

A integração destes conjuntos de atividades é obtida por meio da implantação/utilização de disciplinas transversais, ou seja, tarefas de planejamento, gestão e controle, como governança, gerência de projetos, gestão de processos e outras.

2 Situação da Segurança da Informação e Comunicações

2.1 Comitê de Segurança da Informação e Comunicações - CSIC

Conforme recomendações da IN01, Normas Complementares de Segurança da Informação e Comunicações e Levantamento acerca da Governança de Tecnologia da Informação, publicadas pelo GSI/PR e TCU, o Ministério do Turismo deverá estar aderente às melhores práticas com o objetivo de promover a cultura de Segurança da Informação e Comunicações no Órgão.

O Ministério do Turismo institucionalizou através da Portaria Nº 344, de 26 de outubro de 2012, o Comitê de Segurança da Informação e Comunicações – CSIC e este, deliberou positivamente sobre a Minuta da Política de Segurança da Informação e Comunicações do MTur. A instituição desse Comitê foi o primeiro passo na direção da efetiva Gestão de Segurança da Informação e Comunicações, sendo que esta trata do conjunto de ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança

cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação.

O CSIC é a instância estratégica responsável por tratar e deliberar a respeito de temas na área de Segurança da Informação e Comunicações no âmbito do Ministério do Turismo, observadas as diretrizes de Política de Segurança da Informação e Comunicações estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR. E, para tanto, possui significativa representação de áreas do Ministério, conforme descrito abaixo:

- Secretário-Executivo- SE;
- Chefe de Gabinete do Ministro - GM;
- Consultor Jurídico - CONJUR;
- Secretário Nacional de Políticas de Turismo - SNPTur;
- Secretário Nacional de Programas de Desenvolvimento do Turismo - SNPDTur;
- Diretor de Gestão Estratégica - DGE;
- Diretor de Gestão Interna - DGI;
- Coordenador-Geral de Tecnologia da Informação - CGTI;
- Ouvidor.

Além disso, o CSIC instituiu em seu Regimento Interno, publicado através da Resolução Nº 2, de 13 de novembro de 2012, o Gestor de Segurança da Informação e Comunicações cuja competência foi atribuída ao Coordenador-Geral de Tecnologia da Informação do Ministério do Turismo. Entre suas atribuições, estão:

- Promover cultura de Segurança da Informação e Comunicações;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- Propor recursos necessários às ações de Segurança da Informação e Comunicações;
- Coordenar o CSIC e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
- Realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na Segurança da Informação e Comunicações;

- Manter contato direto com o Departamento de Segurança da Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI/PR para o trato de assuntos relativos à Segurança da Informação e Comunicações;
- Propor normas relativas à Segurança da Informação e Comunicações;
- Apoiar técnica e administrativamente as reuniões e demais atividades do Comitê, incluindo o acompanhamento da execução das resoluções do CSIC;
- Receber e expedir correspondências e comunicados;
- Selecionar e organizar a legislação e a jurisprudência relativas à Segurança da Informação e Comunicações;
- Preparar atos a serem baixados pelo Presidente;
- Informar sobre a tramitação de processos;
- Providenciar:

  a) elaboração e apresentação das propostas a serem discutidas e homologadas nas reuniões do Comitê;

  b) comunicados e demais documentos administrativos.
- Adotar providências para:

  a) realização das reuniões, secretariando-as e elaborando as respectivas atas;

  b) cumprimento das deliberações do Comitê; e

  c) organizar, disponibilizar e manter atualizado o acervo documental correspondente;
- Exercer outras atribuições administrativas que lhe forem conferidas pelo Presidente.

2.2 Grupo de Trabalho de Segurança da Informação e Comunicações – GT-SIC

Em sincronismo com o Planejamento Estratégico do Órgão, na busca da "*Excelência Administrativa*", cujo um dos objetivos é "*Aperfeiçoar o controle interno, a gestão de riscos e a segurança institucional*", em seu projeto "*Aperfeiçoar a Gestão da Segurança da Informação e Comunicações*", foi constituído o Grupo de Trabalho de Segurança da Informação e Comunicações – GT-SIC, conforme Resolução Nº 03, de 29 de maio de 2013, vinculado ao Comitê de Segurança da Informação e Comunicações – CSIC, com caráter consultivo e será responsável para tratar de temas e propor soluções específicas sobre Segurança da Informação e

Comunicações no âmbito do Ministério do Turismo, observadas as diretrizes estabelecidas pelo Departamento de Segurança da Informação e Comunicações do GSI/PR.

Assim sendo, esse Plano Diretor de Segurança da Informação e Comunicações possibilitará a efetiva Gestão de Segurança da Informação e Comunicações no MTur.

2.3 Política de Segurança da Informação e Comunicações - POSIC

Atento às suas responsabilidades e atendendo a demanda legal, o MTur publicou no D.O.U a Política de Segurança da Informação e Comunicações – POSIC, através da Portaria Nº 108 de 22 de maio de 2013, cujo objetivo é implantar diretrizes, responsabilidades, competências e princípios de Segurança da Informação e Comunicações - SIC no âmbito do Ministério do Turismo. E tem como propósito limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade - DICA das informações que suportam os objetivos estratégicos deste Ministério, bem como a conformidade, padronização e normatização das atividades de Gestão de Segurança da Informação e Comunicações do Ministério do Turismo - MTur.

As diretrizes de Segurança da Informação e Comunicações – SIC devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura do MTur. Assim como, a Gestão de Segurança da Informação e Comunicações – GSIC deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SIC.

A publicação da POSIC permitiu ao Ministério conformidade à Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008 e a outras legislações e regulamentações Federais, bem como aderência às melhores práticas de mercado referentes ao tema.

2.4 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR

O gerenciamento de incidentes de segurança em redes de computadores requer especial atenção da alta administração do MTur, pois manter a Segurança da Informação e Comunicações de uma organização em um ambiente computacional interconectado nos dias atuais é um grande desafio, que se torna mais difícil à medida que são lançados novos produtos para a Internet e novas ferramentas de ataque são desenvolvidas.

A criação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR está prevista no Planejamento Estratégico do MTur, em seu projeto "*Aperfeiçoar a Gestão da Segurança da Informação e Comunicações*", será composta por um grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, tem como objetivo definir o processo e as atividades para o correto tratamento de incidentes, com foco na identificação, análise, avaliação e tratamento. E ainda, proporcionar a capacidade de resposta aos incidentes de forma unificada.

O Gestor de Segurança da Informação e Comunicações será responsável por coordenar a instituição, implementação e manutenção da infraestrutura necessária à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do MTur, conforme diretrizes descritas no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008.

2.5 Classificação da Informação

Ainda, em sincronismo com o Planejamento Estratégico do Órgão, na busca da "*Excelência Administrativa*", cujo um dos objetivos é "*Aperfeiçoar o controle interno, a gestão de riscos e a segurança institucional*", em seu projeto projeto "*Aperfeiçoar a Gestão da Segurança da Informação e Comunicações*", será desenvolvida em 2013 a Política de Classificação da Informação cujo objetivo é proteger adequadamente as informações, de propriedade do MTur ou sob sua custódia, contra revelação, adulteração e destruição.

A Norma de Classificação da Informação será composta por regras que orientam o tratamento a ser dado às informações em todo seu ciclo de vida: criação, manipulação, transporte, armazenamento e descarte, categorizando-as de acordo com a sua relevância, e deverá ser baseado Decreto nº 7.845, de 14 de novembro de 2012, na qual regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

3 Situação Atual

3.1 Contexto Inicial

O MTur através do Gestor de SIC, por meio de um trabalho conjunto com o Núcleo de SIC da CGTI, para atender as necessidades do Órgão com relação a Segurança da Informação e considerando a Norma Complementar Nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012 e demais Normas de SIC, realizou o

levantamento da situação atual do Órgão em relação à aderência da SIC. Após o Inventário e Mapeamento dos Ativos de Informação foram realizadas análise e consolidação das informações, contemplando uma proposta de Análise e Avaliação de Riscos para o Plano Diretor de Segurança da Informação e Comunicações do Ministério do Turismo, inicialmente realizado na Coordenação-Geral de Tecnologia da Informação – CGTI.

3.2 Inventário e Mapeamento dos Ativos de Informação

A Norma Complementar Nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, estabelece diretrizes para o processo de Inventário e Mapeamento dos Ativos de Informação, para apoiar a Segurança da Informação e Comunicações, dos órgãos e entidades da APF.

Seguindo essas diretrizes o MTur realizou o Inventário e Mapeamento dos Ativos de Informação da CGTI. A metodologia aplicada na elaboração do Inventário e Mapeamento considerou as informações levantadas nas análises de documentos administrativos, organizacionais e de ativos de Tecnologia da Informação. Também foram consideradas as informações obtidas por meio das entrevistas com os analistas e técnicos dos processos de TI e dados dos projetos já realizados.

As informações coletadas ajudaram a definir as principais necessidades dos Ativos de Informação do Ministério do Turismo e os pontos a serem contemplados no PDSIC. Por ser um processo interativo e evolutivo, o Inventário e Mapeamento foi composto por 04 (quatro) etapas, detalhadas a seguir: Identificação e Classificação dos Ativos de Informação, Identificação dos Riscos, Estimativa dos Riscos e Avaliação de Riscos.

3.2.1 Identificação e Classificação dos Ativos de Informação

Segundo o Guia de referência para a Segurança das Infraestruturas Críticas da Informação "*o processo de Identificação e Classificação dos Ativos de Informação auxilia a organização a conhecer, valorizar, proteger e manter seus recursos em conformidade com os requisitos legais e do negócio*". Para a etapa de Identificação e Classificação dos Ativos de Informação foram seguidas as etapas recomendadas pela Norma Complementar Nº 10: coleta de informações gerais dos ativos de

informação; detalhamento dos ativos de informação; identificação do(s) responsável(is) – proprietário(s) e custodiante(s) de cada ativo de informação; caracterização dos contêineres dos ativos de informação; definição dos requisitos de segurança da informação e comunicações; e estabelecimento do valor do ativo de informação.

3.2.1.1 Coleta de Informações Gerais dos Ativos de Informação

A estratégia para a coleta de informações gerais baseou-se no levantamento e análise de documentos administrativos e de ativos de Tecnologia da Informação. Também foram consideradas as informações obtidas por meio das entrevistas com os analistas e técnicos dos processos de TI e dados dos projetos já realizados.

O Núcleo de SIC da CGTI realizou a coleta dos ativos de informações no primeiro trimestre de 2013, e pela evolução natural dos recursos da informação os perfis gerados pelo mapeamento deverão ser atualizados semestralmente ou sempre que necessário. Com isso, o Comitê de SIC terá o Inventário e Mapeamento dos Ativos de Informação atualizados e com garantia de continuidade e conhecimento sobre os recursos.

A coleta foi embasada nos objetivos estratégicos do MTur e teve como escopo de trabalho a realização do levantamento da situação atual da Coordenação-Geral de Tecnologia da Informação. A Classificação dos Ativos de Informação abrangidos é demonstrada conforme Tabela 3:

CATEGORIA DOS ATIVOS DE INFORMAÇÃO
HUMANOS
INFRAESTRUTURA
APLICAÇÕES
SERVIÇOS

Tabela 3 – Categoria dos Ativos de Informação

3.2.1.2 Detalhamento dos Ativos de Informação

Seguindo a metodologia para a Identificação e Mapeamento dos Ativos de Informação, esta etapa definiu o nível de profundidade das informações coletadas, a partir da necessidade do negócio e dos objetivos estratégicos do MTur. A definição consistente desses ativos ajudou a reduzir a complexidade na coleta das informações.

3.2.1.3 Identificação do(s) Responsável(s) – proprietário(s) e custodiante(s) de cada Ativo de Informação

De acordo com a Norma Complementar Nº 10/IN01/DSIC/GSIPR "*o proprietário do ativo de informação refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação*". E ainda cita que:

> *O proprietário do ativo de informação deve assumir, no mínimo, as seguintes atividades: 1) descrever o ativo de informação; 2) definir as exigências de segurança da informação e comunicações do ativo de informação; 3) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários; 4) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo; e, 5) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação.*

Para os custodiantes dos ativos de informação, a Norma Complementar Nº 10 estabelece que:

> "*O custodiante do ativo de informação deve proteger um ou mais ativos de informação do órgão ou entidade da APF, como é armazenado, transportado e processado, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. Ou seja, deve proteger os contêineres dos ativos de informação, e, consequentemente, aplicar os níveis de controles de segurança conforme as exigências de segurança da informação e comunicações, comunicadas pelo(s) proprietário(s) do(s) ativo(s) de informação*".

Em continuação a Coleta de Informações Gerais dos Ativos de Informação foi realizada a identificação dos responsáveis pelos ativos de informação mapeados.

3.2.1.4 Caracterização dos Contêineres dos Ativos de Informação

Conforme a Norma Complementar Nº 10 "*contêiner é o local onde "vive" o ativo de informação, e assim, recomenda-se que o mesmo seja caracterizado, no mínimo, com as seguintes informações: lista de todos os*

recipientes em que um ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes".

Num processo de avaliação de riscos, a identificação dos contêineres é essencial para identificar os riscos associados à informação. Pois, a proteção e a segurança do ativo de informação dependem do nível de controle implementado no contêiner; o grau de proteção e segurança do ativo depende da eficácia dos controles implementados no contêiner e o quanto tais controles são alinhados com os requisitos exigidos pelo ativo; o ativo de informação herda quaisquer riscos os quais está sujeito seu contêiner. Desta forma, quando se avalia riscos para um recurso de informação, as vulnerabilidades de seu contêiner devem ser consideradas.

3.2.1.5 Consolidação da Identificação e Classificação dos Ativos de Informação mapeados

A Tabela 4 consolida as informações identificadas e classificadas seguindo as recomendações das Normas de Segurança conforme descritos no item 3.2.1 e seus subitens 3.2.1.1 a 3.2.1.4 desse PDSIC:

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
HUMANOS	**Direção e Assessoramento Superior (DAS)**	Servidores de cargo efetivo ou de confiança.	Célia Alves de Melo / COGEP Ramal: 7500	Sala 1003
	Servidores efetivos de Nível Superior	Servidores efetivos de nível superior.	Célia Alves de Melo / COGEP Ramal: 7500	Sala 1003
	Servidores efetivos de Nível Médio	Servidores efetivos de nível médio.	Célia Alves de Melo / COGEP Ramal: 7500	Sala 1003
	Servidores efetivos cedidos (Analistas de TI)	Servidores efetivos cedidos pelo MPOG (ATI's)	Ministério do Planejamento, Orçamento e Gestão / MPOG	Esplanada dos Ministérios Bloco C e K
	Contratos temporários	Trabalho prestado por pessoa física a uma empresa para atender à necessidade transitória de substituição de seu pessoal ou devido ao acréscimo extraordinário de serviços.	Célia Alves de Melo / COGEP Ramal: 7500	Sala 1003
	Estagiários	Atividade prestada comumente por estudantes, nas repartições públicas, visando o aprimoramento profissional.	Simone Maria da Silva Salgado Ramal: 7140	Sala 7140
	Prestadores de Serviços	Trabalho realizado por terceiros.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala 1002
INFRAESTRUTURA	**Servidores Físicos**	Sistema de computação centralizada que fornece serviços a uma rede de computadores.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID – Esplanada / Datacenter – Algar
	Servidores Virtuais	A virtualização permite que várias máquinas virtuais sejam executadas em um único servidor físico.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID – Esplanada / Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	Storages	Solução integrada que lhe permite armazenar, entregar e administrar o conteúdo e as informações em rede de modo que lhe permita.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura - ID/Datacenter - Algar
	Micro-computadores	Computador capaz de variados tipos de tratamento automático de informações ou processamento de dados.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID)
	Notebooks	Computador portátil, leve, designado para poder ser transportado e utilizado em diferentes lugares com facilidade.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID) e Externo
	Impressoras	Periférico com a função de dispositivo de saída, imprimindo textos, gráficos ou qualquer outro resultado de uma aplicação.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID)
	Grupo Gerador	Converte energia mecânica em elétrica.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Subsolo Shopping - ID
	No-breaks	Regula a voltagem e a pureza da energia que chega até os eletrônicos conectados e é responsável por alimentar os dispositivos, em caso de queda de luz, através de uma bateria.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID - Esplanada
	Central Telefônica (IP)	Central telefônica é o equipamento eletrônico que realiza a ligação (comutação) entre dois usuários. Telefonia IP é o roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet, tornando a	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID - Esplanada

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		transmissão de voz mais um dos serviços suportados pela rede de dados.		
	Aparelhos telefônicos (IP)	Aparelho com o conforto e praticidade do telefone com os benefícios da tecnologia IP.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID)
	Racks de Servidores	Rack para servidor é uma espécie de gabinete metálico que possui padronização.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID - Esplanada
	KVM	Gerenciamento de Console Serial.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID - Esplanada
	Equipamento - Solução Segurança	Solução de segurança é a proteção de bens, físicos e lógicos, contra o acesso não autorizado, roubo ou danos.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura - ID
	Data Routers	Roteador vai escolher a melhor rota para o pacote de dados para que você receba as informações rapidamente. Eles podem ser utilizados para ligar dois computadores diferentes ou para ligar dois computadores na Internet.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID - Esplanada
	Estabilizadores	São equipamentos eletrônicos responsáveis por corrigir a tensão da rede elétrica para fornecer aos equipamentos uma alimentação estável.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno
	Switchs	Dispositivos que filtram e encaminham pacotes entre segmentos de redes locais, operando na camada de enlace (camada 2) do modelo OSI.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID - Esplanada

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	Access Points (Aps)	Dispositivo em uma rede sem fio que realiza a interconexão entre todos os dispositivos móveis.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura - ID
	Links	Ligação entre documentos na Internet. Podem ser ligações de um texto para outro texto, imagem, som ou vídeo (ou vice-versa). Um clique em um LINK te conduzirá automaticamente para o documento "*linkado*" (ligado). Atalho.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur/Infovia/ Empresas Externas
APLICAÇÕES	**Blog do Turismo (ASCOM)**	CMS para gerenciar do conteúdo de Blog postado pela ASCOM.	Amanda Kalil M Lavor/ASCOM	Datacenter - Algar
	INTRANET	CMS para gerenciar o conteúdo interno do MTur, conteúdo gerenciado pela ASCOM.	Amanda Kalil M Lavor/ASCOM	Sala Segura - ID
	PGTur (Turismo) - Acessado pelos usuários que encontram-se fora da rede do MTur	PGTur (Plataforma de Gestão do Turismo) tem como função realizar a gestão integrada e informatizada para apoio a administração, integrando o controle de informações de logística de operações, funções e programas, projetos, serviços e demandas em um único sistema, no âmbito do Ministério do Turismo.	Leonardo Schuch/ CGTI Ramal: 7599	Datacenter - Algar
	Central de Informações (ci.pgtur.turismo.gov.br) - Acessado pelos usuários que	A Central de Informações da PGTur, tem como função prover a geração de relatórios customizados ou não. Esta ferramenta é disponibilizada a todos os usuários da PGTur.	Leonardo Schuch /CGTI Ramal: 7599	Sala Segura - ID

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	encontram-se fora da rede do MTur			
	MTurDoc	Sistema de protocolo para tramitação de documentos e processos do MTur.	Paulo Roberto S Lemos/CGTI Ramal: 7575	Sala Segura
	SICA	Sistema de controle e autenticação de usuários do MTur.	Paulo Roberto S Lemos/CGTI Ramal: 7575	Datacenter - Algar
	SISAGM	Sistema de gestão de agenda do ministro segmentado por eventos, audiências e convites.	-	Datacenter - Algar
	DIGITUR	Sistema de digitalização de arquivos.	Maria Luiza Bueno Benevides/CGRL Ramal: 7548	Sala Segura - ID
	Sistema de Sistemas	Sistema de gestão do cadastro do convenente e a inserção de evidências da realização do convênio. Além de realizar o gerenciamento das Aplicações desenvolvidas para o Ministério do Turismo bem como do Hardware e Software adquiridos e disponibilizados pelo Ministério.	Paulo Roberto S Lemos/CGTI Ramal: 7575	Datacenter - Algar
	PRONATEC (Copa)	Sistema para realizar o gerenciamento dos cadastros, possibilitando o público em geral se matricularem nos cursos de capacitação para a COPA 2014. (Programa Nacional de Acesso à Escola Técnica e ao Emprego do Governo Federal).	Paloma Campos Nascimento Salomão/DCPAT Ramal: 7626	Datacenter - Algar
	SADP - Passagens	Sistema para realizar o gerenciamento do cadastramento de bilhetes de passagens e a	Renato Fernandes/CEOF Ramal: 7540	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		conferência da fatura, além de realizar o controle de reembolso.		
	SADP - Diárias	Sistema para realizar o controle de diárias.	Renato Fernandes/CEOF Ramal: 7540	Datacenter - Algar
	Ouvidoria	Sistema para realizar o gerenciamento o cadastro e o acompanhamento de demandas, além de permitir disparar automaticamente alerta, por e-mail, sobre o vencimento do prazo para responder a demanda.	Raimundo Machado dos Santos/Ouvidoria Ramal: 8002	Datacenter - Algar
	SGDTur	Sistema para realizar o gerenciamento o cadastro e o acompanhamento de demandas, além de permitir disparar automaticamente alerta, por e-mail, sobre o vencimento do prazo para responder a demanda.	Paulo Roberto S Lemos/CGTI Ramal: 7575	Datacenter - Algar
	Repasse - Sistema de Acompanhamento de Repasse Público	Esse site apenas apresenta todos os Contratos de Repasse do MTUR e possui uma busca simples sendo aberto para todos.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Datacenter - Algar
	Repasse - Sistema de Acompanhamento de Repasse do MTUR	O Repasse proporciona uma visão gerencial detalhada de todos os contratos de repasse firmados entre a CEF e o MTur desde 2001.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	SIACOR - Sistema de Acompanhamento de Repasse (Casa Civil)	O SIACOR proporciona uma visão gerencial detalhada de todos os contratos de repasse firmados entre a CEF e demais ministérios incluindo o MTUR. Sistema praticamente igual	-	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		ao REPASSE, porém com algumas alterações disponibilizadas para a Casa Civil.		
	Monitoramento de desempenho	Portal de monitoramento de desempenho do MTur.	Luís Henrique Fanan/DGE Ramal: 7102	Datacenter - Algar
	Portal de Acesso a Informação	O objetivo da Lei de Acesso à informação é oferecer ao cidadão um padrão uniforme de acesso, que facilite a localização e obtenção das informações e se torne para ele, também, uma referência em transparência pública.	Raimundo Machado dos Santos/Ouvidoria Ramal: 8002	Datacenter - Algar
	Sistema de Acompanhamento de demandas	Controle de demandas, prazos e custos dos trabalhos realizados pelas agências de publicidade que atendem o Ministério do Turismo.	Sérgio Flores de Albuquerque/Marketing Ramal: 7970	Datacenter - Algar
	CDE - Sistema de Controle das Demandas Externas	O CDE foi concebido com a intenção de prover a rastreabilidade das demandas oriundas de órgãos externos que foram endereçadas a SE.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	CDSE - Sistema de Controle das Demandas de Reuniões	O CDSE foi concebido com a intenção de prover a rastreabilidade das demandas de reuniões organizadas pela SE.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	Radar - Radar Executivo	A aplicação RADAR foi concebida para acompanhar os temas internos da Secretaria Executiva e seus desdobramentos.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	Organograma - Sistematização do	O organograma apresentado se baseia nas informações prestadas pelo RH na plataforma de gestão PGTUR.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	Organograma do Ministério do Turismo			
	Painel PNT - Painel dos Grandes Números do Turismo	Nesse sistema, que se apresenta em um painel, estão os grandes números estatísticos do turismo com foco nos resultados a serem alcançados no PNT.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	Copa do Mundo 2014 - Sistema de controle das ações do Ministério na Copa do Mundo 2014	Sistema responsável em registrar as ações do Ministério para a preparação do País para a Copa do Mundo 2014, além de prover um ambiente de disponibilização de informações institucionais.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	Agenda Competitividade - Sistema de controle de pleitos do setor do turismo	Sistema responsável em registrar e acompanhar os pleitos do setor, mantendo um histórico das ações decorrentes, bem como seus resultados.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	Propostas SICONV - Painel de acompanhamento das propostas cadastradas no SICONV	Sistema concebido para o acompanhamento do cadastramento das propostas no SICONV.	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	GPWEB	Sistema para gerenciamento de demandas internas da CGTI	Sérgio Braune Solon de Pontes /SE Ramal: 7111	Sala Segura - ID
	CONSIAFI	Sistema para gerenciamento de consultas ao SIAFI.	Deusivaldo Ferreira de Jesus/CGPOF	Sala Segura - ID

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
			Ramal: 7313	
	Onde se hospedar	Site que dará direcionamento aos turistas na Copa de hospedagem tanto no CADASTUR como em outros hotéis.	Sergio Flores de Albuquerque / CGMP Ramal: 7970	Datacenter - Algar
	Painel de Controle do Ministro - PCM	Sistema de acompanhamento de emendas parlamentares, acompanhamento da execução de convênios, contratos de repasse e termos de parceria derivados de emenda ou programação. Produção de relatórios gerenciais e geração de indicadores de gestão.	-	-
	SIAAD	Sistema para gestão das demandas recebidas pela AECI, integrado ao MTurDoc, centralizando as informações sobre convênios da AECI com a base de dados do Ministério do Turismo. Ferramenta capaz de realizar todas as atividades relacionadas ao tratamento dos convênios e demandas (denúncias ou solicitações).	Ricardo Cardoso dos Santos/AECI Ramal: 7081	Em Desenvolvimento
	CADASTUR	Cadastro de prestadores de Serviços Turísticos e Guias em Turismo. Sistema de cadastro via internet das empresas prestadoras de serviços turísticos.	Jair Galvão Freire Neto/CGQT Ramal: 8100	Datacenter - Algar
	CertifyTur	Modulo de assinatura digital para emissão de certificados de cadastro do CADASTUR e SBCLASS.	Jair Galvão Freire Neto/CGQT Ramal: 8100	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	SBClass	O Sistema Brasileiro de Classificação estabeleceu sete tipos de Meios de Hospedagem, para atender a diversidade da oferta hoteleira nacional (Hotel, Resort, Hotel Fazenda, Cama & Café, Hotel Histórico, Pousada e Flat/Apart-Hotel) e utiliza a consagrada simbologia de estrelas para diferenciar as categorias.	Jair Galvão Freire Neto/CGQT Ramal: 8100	Datacenter - Algar
	Fiscalização	O Sistema que será utilizado pelo Ministério do Turismo e seus órgãos delegados para fiscalizar os prestadores de serviços turísticos. (De acordo com a Lei nº 11.771 de 17 de setembro de 2008, e do Decreto nº 7.381, de 2 de dezembro de 2010).	Jair Galvão Freire Neto/CGQT Ramal: 8100	-
	INVTUR	Sistema de Inventariação da Oferta Turística. Levantamento, identificação e registro dos atrativos turísticos, dos serviços e equipamentos turísticos e da infraestrutura de apoio ao turismo como instrumento base de informações para fins de planejamento e gestão da atividade turística.	Jun Alex Yamamoto/Regionalização Ramal: 8130	Datacenter - Algar
	INVTUR 2.0	Manutenção Evolutiva do Sistema de Inventariação da Oferta Turística. Levantamento, identificação e registro dos atrativos turísticos, dos serviços e	Jun Alex Yamamoto/Regionalização Ramal: 8130	-

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		equipamentos turísticos e da infraestrutura de apoio ao turismo como instrumento base de informações para fins de planejamento e gestão da atividade turística.		
	BOH	Sistema com metodologia unificada de apuração das informações sobre a ocupação hoteleira e perfil de hóspedes em meios de hospedagem em todas as Unidades da Federação - UFs, com validade e comparabilidade de dados nas instâncias administrativas nacional, regional, estadual e municipal.	Jair Galvão Freire Neto/CGQT Ramal: 8100	Datacenter - Algar
	FISCON	Fiscalização de convênios para eventos geradores de fluxo, Sistema de fiscalização e acompanhamento de convênios firmados com o MTur – FISCON.	Soemes Castilho da Silva/CGMC Ramal: 7116	Datacenter - Algar
	GEOTUR (Sistema Georeferenciado do Turismo)	Sistema cedido pelo Ministério do Meio Ambiente disponibiliza informações geográficas e georeferenciadas de demonstração das informações alimentadas pelo PRTUR, CADASTUR, INVTUR e SIGTUR.	Fábio Monteiro Rigueira/DEPAT Ramal: 7738	Datacenter - Algar
	Indicadores	Indicadores para acompanhamento das metas do plano nacional do turismo – PNT.	Fábio Monteiro Rigueira/DEPAT Ramal: 7738	Datacenter - Algar
	PRTUR	Sistema de gerenciamento de informações do Programa de Regionalização do Turismo.	Jun Alex Yamamoto/Regionalização	Datacenter - Algar

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
			Ramal: 8130	
	REDREG	Trata-se de uma ferramenta eletrônica de troca de informações na qual participantes, previamente inscritos, trocam mensagens entre si nos fóruns de discussão. Através da Redereg é possível o Grupo Gestor marcar reuniões, criar tópicos para discussão e, até mesmo, trocar mensagens instantaneamente por meio da ferramenta "reuniões". Além disso, somente o Grupo Gestor terá acesso a seu respectivo Destino, mantendo assim, todas as informações ali postadas em segurança. Diariamente, o Ministério do Turismo divulga projetos e notícias de interesse dos Grupos dos 65 Destinos Indutores, estabelecendo, assim, um canal de comunicação com os mesmos.	Jun Alex Yamamoto/Regionalização Ramal: 8130	Em reformulação
	SIGTUR	Sistema Integrado de Gestão do Turismo, que é alimentado, em tempo real, por informações sobre o estágio dos programas previstos no PNT (Plano Nacional de Turismo) e pela execução físico-orçamentária do PPA (Plano Plurianual). O sistema é também um método de gestão, que armazenar o conteúdo do PNT e acompanha as ações de turismo e seus respectivos reflexos sobre as metas governamentais para o turismo.	Fábio Monteiro Rigueira/DEPAT Ramal: 7738	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	SISEM	Controle de propostas e dos saldos das emendas parlamentares.	Bernardo de Castro Soares/CGAP Ramal: 7965	Datacenter - Algar
	BBE (ambiente de homologação)	É uma ferramenta de tecnologia para pesquisa, por meio de um sistema de gestão de Banco de Dados de Eventos e Ações de Sensibilização de Promotores de Eventos, proporcionando à cadeia produtiva do turismo brasileiro informações estratégicas que possibilitam o planejamento anual das ações de captação de eventos e ordenamento de novos destinos brasileiros de Negócios e Eventos.	Wilken Souto/CGSG Ramal: 8190	Sala Segura - ID
	SIMT	Estimativa da mão de obra dos segmentos de turismo a partir da RAIS, CAGED, PINAD, fornece dados facilitadores para formulação de políticas públicas que incentivem o turismo.	Neiva Aparecida Duarte / DEPES Ramal: 8241	Datacenter - Algar
	SG65	O Sistema foi especialmente criado para auxiliá-lo na gestão e monitoramento das ações discutidas pelo Grupo Gestor e possui dois módulos como ferramenta de gestão, o Monitoramento de Ações e o Painel de Indicadores.	Jun Alex Yamamoto/Regionalização Ramal: 8130	Sala Segura - ID
	SICET	Sistema de informações referentes aos Fóruns e Conselhos Estaduais de Turismo, alimentado de forma descentralizada pelos secretários-executivos dos colegiados estaduais, disponíveis	Fábio Monteiro Rigueira/DEPAT Ramal: 7738	Datacenter - Algar

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		tanto para os conselheiros como para o público em geral.		
	SNRHos (é um módulo da PGTur)	O SNRHos (Sistema Nacional de Registro de Hóspedes) é o sistema criado pelo MTur para informatizar a Ficha Nacional de Registro de Hóspedes – FNRH, facilitando o envio, pelos meios de hospedagem, das informações exigidas pela Lei. Este sistema permite que o governo federal realize o tratamento dessas informações identificando o perfil do turista e as taxas de ocupação hoteleira de cada região, possibilitando a melhoria da elaboração de políticas públicas direcionadas ao setor turístico.	Fernanda Carneiro / CGQT Ramal: 8217	Datacenter - Algar
	Marketing	Viabilizar o controle das Planilhas de Propostas de Ações de Divulgação (PAD) geradas e enviadas à SECOM, Ordens de Serviço emitidas e processos de pagamentos.	Sergio Flores de Albuquerque / CGMP Ramal: 7970	Sala Segura - ID
	Portal Institucional (Turismo institucional)	Portal oficial de divulgação das ações, programas, notícias, legislação, estrutura administrativa do MTur.	Sergio Flores de Albuquerque / CGMP Ramal: 7970	Datacenter - Algar
	Turismo Brasil (Hotsite Promocional)	Promoção dos destinos turísticos brasileiros (principalmente dos 65 destinos indutores e 87 roteiros turísticos). Fotos, vídeos e comentários das regiões turísticas do Brasil como clima,	Jun Alex Yamamoto/Regionalização Ramal: 8130	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		mapas, acessos rodoviários, distâncias e telefones úteis.		
	Eventos	Divulgação dos principais eventos culturais, folclóricos, religiosos, cívicos e esportivos do país.	Wilken Souto/CGSG Ramal: 8190	Datacenter - Algar
	Viaje Legal	Hotsite com dicas e informações sobre cuidados que turista deve tomar com a bagagem, com a saúde, locação de veículos, compras de pacotes, hospedagem, dentre outros.	Isabel Cristina Barnasque/CGIN Ramal: 8110	Datacenter - Algar
	Salão do Turismo	Promocional do evento Salão do Turismo; o evento, datas, realização, estrutura, programação, e informações sobre as edições passadas.	Isabel Cristina Barnasque/CGIN Ramal: 8110	Datacenter - Algar
	Dados e Fatos	Site que apresenta os estudos, pesquisas, dados estatísticos e análises sobre o desempenho da atividade turística no país.	Neiva Aparecida Duarte / DEPES Ramal: 8241	Datacenter - Algar
	Viaja Mais Melhor Idade	Hotsite que promove o programa Viaja Mais Melhor Idade, trazendo informações institucionais sobre o programa.	Wilken Souto/CGSG Ramal: 8190	Datacenter - Algar
	Hotsite SBClass	Divulgação do novo sistema de classificação dos Meios de Hospedagem.	Jair Galvão Freire Neto / DEAT Ramal: 8100	Datacenter - Algar
	Hotsite Destinos Referência	Site para realizar a divulgação dos destinos através da internet, bem como divulgar o material produzido no âmbito do projeto para outros destinos turísticos.	Wilken Souto/CGSG Ramal: 8190	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	Banco de Vídeos	Local utilizado para download de vídeos. Para suprir as demandas do banco de vídeo.	Sergio Flores de Albuquerque / CGMP Ramal: 7970	Datacenter - Algar
	Portal do Sistema Nacional de Registros de Hospedes	O Sistema Nacional de Registro de Hóspedes – SNRHos é o sistema criado pelo Ministério do Turismo – MTur , para informatizar a Ficha Nacional de Registro de Hóspedes – FNRH, facilitando o envio, pelos meios de hospedagem, das informações exigidas pela Lei 11.771/2008 e Decreto 7.381/2010, permitindo que o governo federal realize o tratamento dessas informações identificando o perfil do turista e as taxas de ocupação hoteleira de cada região, possibilitando a melhoria da elaboração de políticas públicas direcionadas ao setor turístico.	Jair Galvão Freire Neto / DEAT Ramal: 8100	Datacenter - Algar
	Portal de Consulta Pública	Programa de Regionalização do Turismo Módulo Consulta Pública.	Jun Alex Yamamoto/Regionalização Ramal: 8130	Datacenter - Algar
	Destinos em Referência em Segmentos Turísticos	Divulgação do projeto "Destinos em Referência em Segmentos Turísticos", que visa o desenvolvimento de um destino por meio de um segmento, partindo do princípio de que o trade local deve estar organizado, com prioridades e	Wilken Souto/CGSG Ramal: 8190	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		estratégias definidas e com foco na competitividade.		
	Portal de Competências	O Portal de Competências tem como principal objetivo registrar, conhecer e identificar o potencial humano do Ministério do Turismo, bem como conhecer a formação acadêmica, profissional e as áreas de interesse dos servidores.	Célia Alves Melo/COGEP Ramal: 7500	Datacenter - Algar
	65 Destinos Indutores	Blog que promove o projeto 65 Destinos Indutores, que tem como objetivo capacitar os atores locais para a gestão em turismo, ampliar os conhecimentos sobre planejamento estratégico, fortalecer a governança e a inter-relação dos destinos com as regiões em que estão inseridos.	Jun Alex Yamamoto/Regionalização Ramal: 8130	Datacenter - Algar
	SGT	Sistema de Gestão & Planejamento de Destinos Turísticos.	Jun Alex Yamamoto / CGRG Ramal: 8130	Sala Segura - ID
	Turista	Site que receberá usuários diretamente do Qrcode da campanha JMJ e direcionará aos diversos canais do MTur	Ana Lúcia Carrias/CGIN Ramal: 8114	Datacenter - Algar
	Mapa de qualificação	Monitoramento dos cursos de qualificação realizados no âmbito do Bem Receber Copa. O Mapa de Qualificação Profissional mostra quem são os alunos, onde moram e em quais segmentos turístico eles foram treinados.	Marcela Jeolas/DCPAT Ramal: 7600	Sala Segura - ID

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	SIGA	Sistema de gestão acadêmica com a finalidade de monitorar as ações do Bem Receber Copa.	Marcela Jeolas/DCPAT Ramal: 7600	-
	SIT	O Sistema SIT(GESPRO) visa o controle de propostas, convênios, emendas; controle dos documentos (ofícios e memorandos) que entram e que saem da DIETU.	Marcia Beatriz Beiró Lourenço/DIETUR Ramal 7850	Datacenter - Algar
	Bem Receber Copa	Site de divulgação do Programa de qualificação profissional do Ministério do Turismo, em parceria com entidades do setor, para até 2013, por meio de soluções presenciais e a distância, qualificar 306 mil profissionais que trabalhem com a linha de frente de atendimento ao turista.	Marcela Jeolas/DCPAT Ramal: 7600	Hospedado em Externo
	Olá Turista	Site para divulgar o Programa Olá Turista, que oferece 80 mil vagas gratuitas para cursos on-line de inglês e espanhol, com o objetivo de qualificar a recepção do turista estrangeiro para Copa do Mundo de 2014.	-	Hospedado em Externo
	Normalização em Turismo	Disponibilização das normas brasileiras publicadas no âmbito do Comitê Brasileiro de Turismo no MERCOSUL.	Maria Luiza Moreira Nova da Costa/DCPAT Ramal: 7621	Hospedado em Externo
	Turismo Sustentável e Infância	Site de divulgação do projeto Turismo Sustentável e Infância: Sensibilização, no Brasil e no Exterior, para o Enfrentamento da Exploração Sexual infanto-juvenil no Turismo, insere-se como uma nova estratégia para	Adelino Silva Neto/CGTSI Ramal: 7401	Datacenter - Algar

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		reforço das ações já existentes de enfrentamento ao turismo com motivação sexual infanto-juvenil promovidas pelo Ministério do Turismo, com o apoio do Conselho Nacional de Turismo.		
	SIPROTUR – Sistema de Acompanhamento do PRONATEC Turismo	Sistema de comunicação entre as Secretarias Estaduais, Instituições de Ensino (SENAC, SENAI) e o Ministério do Turismo, objetivando a pactuação de vagas para o programa PRONATEC COPA NA EMPRESA.	Paloma Campos Nascimento Salomão/DCPAT Ramal: 7626	Sala Segura - ID
SERVIÇOS	**Acesso Internet**	Provê o acesso à Internet para os funcionários e visitantes do Ministério do Turismo com qualidade e rapidez.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID) e externo
	Comunicação de voz e dados	Provê a comunicação entre a Esplanada e o Shopping ID através de fibras óticas, provendo uma conexão de alto desempenho com capacidade de transportar grandes quantidades de informações com imunidade às interferências eletromagnéticas.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID) e externo
	Conexão WI-FI	Provê o acesso à Internet sem fio no Ministério do Turismo, utilizada mais pelos visitantes, sendo necessário uma senha e o cadastro do *Mac Address* no servidor DHCP, para solicitar esse serviço será necessário chamar o técnico no local.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura / MTur – Interno (Esplanada e ID)

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
	LAN/Cabeamento	Provê a conexão entre as redes de informática e telefonia.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura / MTur – Interno (Esplanada e ID) e externo
	Help Desk	Provê o serviço de apoio a usuários para suporte e resolução de problemas técnicos, restabelecendo a operação normal dos serviços dos usuários do Ministério do Turismo o mais rápido possível. Acessível pelo telefone ***22** ou pelo número **0800 606-8484**.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID) e externo
	Correio Eletrônico	Provê o serviço de comunicação dos funcionários no meio interno e externo com total segurança das informações, com espaço adequado de acordo com a necessidade. Esse serviço é solicitado quando o funcionário ingressa no Ministério do Turismo seja ele: Estagiário, Terceirizado ou Concursado por meio de um formulário de rede autorizado pelo chefe do setor.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Datacenter - Algar
	Telefonia	Provê um serviço de comunicação dos funcionários do Ministério do Turismo no meio interno e externo de acordo com as necessidades para desempenhar o serviço, contando com aparelhos modernos capazes de fazer vídeo conferencia.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura / MTur – Interno (Esplanada e ID)
	Compartilhamento de arquivos	Provê um serviço de armazenamento de dados com total disponibilidade de recursos de	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID / Datacenter Algar

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		interação a usuários ou estações de trabalho, bem como em benefícios de segurança com a criação de florestas, domínios, árvores, Unidades Organizacionais (OUs) e grupos de trabalho.		
	Hospedagem Web	Provê de uma estrutura para hospedagem de páginas do Ministério do Turismo com alta disponibilidade e segurança.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura ID / Datacenter Algar
	Storage Backup	Provê um serviço de armazenamento são centralizadas e totalmente gerenciadas de forma a garantir o melhor benefício no ciclo de vida da informação. E, por meio de modernas políticas automatizadas de proteção da informação (backup), dados críticos do Ministério do Turismo ficam protegidos e disponíveis a qualquer momento em caso de necessidade de restauração,	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura - ID
	Antivírus	Provê um sistema de proteção que se destaca pelo seu excelente desempenho, tudo para verificar e bloquear e-mails perigosos, conteúdo arriscado da internet e ameaças como vírus, cavalos de Tróia, Spywares e Rootkits impedindo que os computadores do Ministério do Turismo sejam Invadidos e envie as	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura - ID

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	DETALHAMENTO	DESCRIÇÃO	RESPONSÁVEL	CONTÊINERES
		informações pessoais para redes e pessoas má intencionadas.		
	Firewall	Provê um sistema de proteção oferendo desempenho e segurança para a rede do Ministério do Turismo, identificando e bloqueando conteúdo de páginas inadequadas para as atividades prestadas pelo órgão e barrando ameaças.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura / MTur – Interno (Esplanada e ID)
	IPS	Provê uma solução de segurança inteligente e exclusiva que descobre e bloqueia ameaças sofisticadas na rede, usando técnicas avançadas de detecção de ameaças, ele vai além da mera correspondência de padrões, defendendo contra ataques ocultos com extrema precisão.	Paulo Roberto S Lemos / CGTI Ramal: 7575	Sala Segura / MTur – Interno (Esplanada e ID)
	Suporte Técnico 0800	Serviço para manutenção de computadores, impressoras, scanner, fax, movimentação dos equipamentos de Informática e Atendimentos no Ministério do Turismo.	Paulo Roberto S Lemos / CGTI Ramal: 7575	MTur – Interno (Esplanada e ID) e externo

Tabela 4 – Consolidação da Identificação e Classificação dos Ativos de Informação mapeados

3.2.1.6 Definição dos Requisitos de Segurança da Informação e Comunicações

Os requisitos de Segurança da Informação e Comunicações dos Ativos de Informação devem ser definidos por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

O MTur deverá possuir, no mínimo, os Requisitos de SIC descritos a seguir para que suas informações sejam adequadamente protegidas:

- **Política de Segurança da Informação e Comunicações**: existência de uma Política de Segurança da Informação atualizada e adequadamente divulgada aos seus colabores;
- **Organização da Segurança da Informação**: área ou pessoa responsável pela coordenação das ações de Segurança da Informação e Comunicações;
- **Gestão de Ativos**: todos os ativos (micro, impressoras, celulares, etc) do Órgão deverão estar controlados e conforme a Política de Segurança da Informação e Comunicações e deverão estar classificados quando for o caso;
- **Segurança em Recursos Humanos**: treinamentos de conscientização em SIC para orientação dos funcionários; toda devolução de ativo deve ser efetivamente controlada; os procedimentos de encerramento e transferência de pessoas devem assegurar a proteção das informações e ativos;
- **Segurança Física**: a entrada física deve ser monitorada através de CFTV; assegurar acesso somente às pessoas autorizadas; o acesso ao público, áreas de entrega e carregamento deve ser efetivamente monitorado; realização de manutenção periódica nos geradores; procedimento formal contendo regras para a alienação ou reutilização de equipamentos; procedimento formal para controle da retirada de equipamentos;

Gerenciamento das Operações e Comunicações: procedimento formal e registro de mudanças significativas no ambiente produtivo; segregação de funções críticas;
topologia de rede que garanta a adequada segregação dos recursos de TI (exemplos: servidores de desenvolvimento, homologação, produção e internet); controle sobre os prestadores de serviços que tratam as informações do MTur; formalização do procedimento operacional para cópias de segurança;
procedimentos de Segurança da Informação sobre eventual rede sem fio, incluindo responsabilidades operacionais sobre a rede, fluxo de solicitação, aprovação, implantação e revisão de regras de Firewall e

roteadores; controle formal sobre as mídias removíveis; descarte seguro de mídias removíveis; controle formal para identificação de todas as mídias com informações sensíveis, conforme política de classificação da informação; procedimento para transporte de mídias; documentação

- contendo o fluxo de recebimento e processamento de informações do MTur; mecanismos de proteção apropriados aos registros dos logs; mecanismo que permita a sincronização dos relógios de computadores a um padrão de tempo confiável;
- **Controle de Acessos**: processo formal de solicitação, concessão e revisão dos direitos de acesso; procedimento formal que identifique e registre todos os privilégios especiais de acesso aos servidores e aplicações destinados as informações do MTur; requisitos mínimos de segurança para senhas: troca periódica de senhas, restrição para reutilização de senhas, criação de máscaras de senhas, nível mínimo de complexidade; existência de uma política de "mesa limpa" para papéis e mídias removíveis, conforme política de segurança da informação; bloqueio de estações em função de inatividade; segregação das redes de comunicação em domínios lógicos protegidos por um perímetro de segurança definido; documentação atualizada contendo a topologia que aborde as diferentes redes segregadas através de *Firewall's* ou roteadores; documentação contendo as regras de permissionamento aos sistemas; documentação relacionada aos sistemas;
- **Gerenciamento de Controles criptográficos e atualizações de paths:** política para o uso de controles de criptografia; ata de Cerimônia das Chaves Criptográficas; documentação atualizada relacionada às atualizações de paths e antivírus das estações e servidores.
- **Gestão de Incidentes de Segurança da Informação**: procedimento formal para tratamento de incidentes de segurança da informação; procedimento formal para análise crítica de incidentes de segurança da informação;
- **Gestão de Continuidade dos Negócios**: procedimento formal para continuidade dos negócios; existência de um Plano de Gestão de Continuidade dos Negócios.

3.2.1.7 Estabelecimento do Valor do Ativo de Informação

Conforme a NBR ISO/IEC 27005:2011 para estabelecer o valor de seus ativos, uma organização precisa primeiro identificá-los (num nível de detalhamento adequado). Dois tipos de ativos podem ser distinguidos:

- **Ativos Primários**:
    - Processos e atividades do negócio;

- Informação.

- **Ativos de Suporte e Infraestrutura** (sobre os quais os elementos primários do escopo se apoiam), de todos os tipos:
  - Hardware;
  - Software;
  - Rede;
  - Recursos humanos;
  - Instalações físicas;
  - A estrutura da organização.

Para este PDSIC foram mapeados os Ativos de Suporte da Coordenação-Geral de Tecnologia da Informação, conforme Tabela 5:

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	TIPO
HUMANOS	**Suporte**
INFRAESTRUTURA	**Suporte**
APLICAÇÕES	**Suporte**
SERVIÇOS	**Suporte**

Tabela 5 – Identificação do Valor dos Ativos de Informação

Seguindo as orientações da NBR ISO/IEC 27005:2011, após a identificação do tipo de ativo, foi determinada a escala de medida a ser usada e os critérios que permitam posicionar um ativo no seu correto lugar nessa escala, em função de seu valor qualitativo, conforme Tabela 6:

CRITÉRIOS	MEDIDA
Muito baixo	1
Baixo	2
Médio	3
Alto	4
Muito alto	5

Tabela 6 – Critérios e medidas

O estabelecimento dos valores dos ativos de informação será útil para a alta administração decidir a respeito, através de uma análise de custo e benefício, dos controles que devem ser utilizados para mantê-lo.

3.3 Identificação dos Riscos

De acordo com a norma NBR ISO/IEC 27005:2011, a primeira etapa da identificação de riscos é a identificação dos ativos. Dentro do escopo do risco, os Ativos de Suporte na CGTI foram listados, tendo em vista o valor para a instituição observado pelas entrevistas com os analistas e técnicos dos processos de TI e dados dos projetos já realizados.

A identificação dos riscos considera as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, estimar os níveis de riscos de modo que eles sejam avaliados e priorizados pelo MTur.

O objetivo da fase de identificação dos riscos é, portanto:

- Identificar os ativos dentro do escopo do Plano Diretor de Segurança da Informação do MTur;
- Identificar as ameaças a esses ativos;
- Identificar as vulnerabilidades que possam ser exploradas por essas ameaças;
- Identificar as consequências e os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos (CID), incluindo-se a autenticidade (A).

3.3.1 Ameaças

As ameaças à Segurança da Informação são relacionadas diretamente à perda de uma de suas 3 características principais, quais sejam:

- **Perda de Confidencialidade**: seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.
- **Perda de Integridade**: aconteceria quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.
- **Perda de Disponibilidade**: acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como *crackers*, (*hackers* não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas). Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, autoestima, vingança e o dinheiro.

As ameaças podem ser classificadas em: (I) **intencionais**, que indica as ações intencionais direcionadas contra os ativos da informação; (A) **acidentais**, que indica as ações de origem humana que podem comprometer acidentalmente e os ativos da organização; ou de origem (N) **natural** ou ambiental, que indica incidentes que não são provocados pela ação dos seres humanos.

A Tabela 7 apresenta as ameaças identificadas para este PDSIC:

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	AMEAÇA	ORIGEM
HUMANOS	*Hacker*, *cracker*	I
	Criminosos digitais	I
	Terroristas	I
	Espiões	I
	Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas	A, I
	Fraude	I
	Arrombamento	I
	Escuta telefônica	I
INFRAESTRUTURA	Fogo	A, I, N
	Água	A, I, N
	Destruição de equipamento ou mídia	A, I, N
	Poeira, corrosão ou congelamento	A, I, N
	Fenômeno sísmico	N
	Fenômeno meteorológico	N
	Inundação	N
	Falha do condicionador de ar	A, I
	Interrupção no suprimento de energia	A, I, N
	Falha do equipamento de telecomunicações	A, I
	Radiação eletromagnética	A, I, N
	Furto de mídia ou documentos	I
	Furto de equipamentos	I
	Recuperação de mídia reciclada ou descartada	I
	Divulgação indevida	A, I
	Alteração de *hardware*	I
	Alteração de *software*	A, I
	Defeito de equipamento	A
	Saturação do sistema de informação	A, I
	Defeito de *software*	A
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	A, I
	Uso não autorizado de equipamento	I
	Cópia ilegal de *software*	I
	Uso de cópias de software falsificadas ou ilegais	A, I

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	AMEAÇA	ORIGEM
	Comprometimento dos dados	I
	Processamento ilegal dos dados	I
	Erro durante o uso	A, I
	Forjamento de direitos	A, I
	Abuso de direitos	I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A, I, N
	Ação de código malicioso	I
APLICAÇÕES	Erro durante o uso	A, I
	Falhas de codificação, *bugs*	A, I
	Abuso de direitos	I
	Ação de código malicioso	A, I
SERVIÇOS	Indisponibilidade de serviços ou informações	A, I, N
	Falta de Apoio às Ações de SIC	A, I
	Não atendimento à regulamentação	A, I
	Acesso lógico não autorizado	A, I
	Acesso indevido a informações confidenciais	A, I
	Ação de código malicioso	A, I
	Dano a pessoas	A, I, N
	Dano à imagem da organização	A, I, N
	Atraso na entrega do serviço	A, I, N
	Perda de qualidade do serviço	A, I
	Falha em meios de comunicação	A, I, N
	Queda de performance	A, I, N

Tabela 7 – Classificação de Ameaças

3.3.2 Vulnerabilidades

De acordo com a Norma Complementar Nº 04/IN01/DSIC/GSIPR os Riscos de SIC "*estão associados à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.* Sendo, *as vulnerabilidades um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação*".

3.3.3 Consequências

A identificação dos riscos considera as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, estimar os níveis de riscos de modo que eles sejam avaliados e priorizados pelo MTur. Para esse PDSIC foram identificadas das ameaças e vulnerabilidades dos Ativos de Informação da Coordenação-Geral de TI e mapeadas as consequências relativas a essa identificação.

3.3.4 Ações de SIC adotadas (Controles de SIC)

Nesta etapa foram identificadas pelo Núcleo de SIC da Coordenação-Geral de TI, de acordo a identificação das ameaças e vulnerabilidades, as ações de segurança da informação já adotadas pelo Ministério do Turismo.

A Tabela 8 demonstra as ameaças, vulnerabilidades, consequências e as ações de SIC identificadas para esse Plano Diretor de Segurança da Informação e Comunicações:

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
HUMANOS	Ausência de recursos humanos	Indisponibilidade de recursos humanos	✓ Sobrecarga de trabalho ✓ Atividades executadas inadequadamente por falta de pessoal	✓ Condução de projeto para elaboração da proposta de criação de cargos de ATI's do MTur, para solicitação ao MPOG
	Procedimentos de recrutamento inadequados	Indisponibilidade de recursos humanos	✓ Falta de qualificação profissional ✓ Profissionais com perfis inadequados para as atividades da área	✓ Condução de projeto para elaboração de Plano de Capacitação. ✓ Redistribuição de atividades de acordo com perfil profissional existente
	Treinamento insuficiente em segurança	Erro durante o uso	✓ Acessos indevidos ✓ Vazamento de informação ✓ Perda de dados ✓ Falta de conhecimento	✓ Condução de projeto para elaboração de Plano de Capacitação
	Uso incorreto de *software* e *hardware*	Erro durante o uso	✓ Perda de dados ✓ Instalações e remoções indevidas ✓ Programas maliciosos ✓ Danificação de equipamento ✓ Sobrecarga de recursos	✓ Compartilhamento de conhecimentos
	Falta de conscientização em segurança	Erro durante o uso	✓ Acessos indevidos ✓ Vazamento de informação ✓ Perda de dados ✓ Falta de conhecimento ✓ Uso inadequado dos ativos de informação	✓ Instituição da Política de Segurança da Informação e Comunicações. ✓ Condução de projeto para elaboração do Plano Diretor de SIC
	Inexistência de mecanismos de monitoramento	Processamento ilegal dos dados	✓ Acessos indevidos ✓ Sobrecarga de link internet ✓ Invasão ✓ Má utilização dos recursos de TI	✓ Utilização de aplicativos de monitoramento (SCCM, EPO, ZABBIX, outros)

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de mídia ou documentos	✓ Acessos indevidos ✓ Perda de dados ✓ Vazamento de informação	✓ Sistema de câmera de segurança. ✓ Controle de acesso físico (recepção setorial)
	Inexistência de políticas pra o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de recurso	✓ Acessos indevidos ✓ Vazamento de informação ✓ Má utilização dos recursos de TI	✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação
	Inexistência de controle de acesso lógico	*Hacker*, *cracker*	✓ *Hacking* ✓ Engenharia social ✓ Negação de serviço ✓ Pichação de sites ✓ Invasão de sistemas, infiltrações ✓ Acesso não autorizado	✓ Antivírus ✓ Firewall
	Inexistência de controle de acesso lógico	Criminosos digitais	✓ Atos virtuais fraudulentos ✓ Intrusão de sistemas ✓ Suborno por informação ✓ Ataques a sistemas	✓ Antivírus ✓ Firewall
	Conflito de interesses	Terroristas	✓ Ataques com bombas ✓ Guerra de informação ✓ Ataques a sistemas ✓ Invasão e dominação de sistemas ✓ Alteração de sistemas	-
	Conflito de interesses	Espiões	✓ Garantir vantagem de um posicionamento defensivo ✓ Garantir uma vantagem política ✓ Exploração econômica ✓ Furto de informações	-

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
			✓ Violação da privacidade das pessoas ✓ Engenharia social ✓ Invasão de sistemas ✓ Invasão de privacidade ✓ Acessos não autorizados em sistemas (acesso a informação restrita, de propriedade exclusiva, e/ou relativa à tecnologia)	
	Conflito de interesses	Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas.	✓ Agressão a funcionário ✓ Chantagem ✓ Busca de informação sensível ✓ Abuso dos recursos computacionais ✓ Fraudes ✓ Furto de ativos ✓ Suborno de informação ✓ Inclusão de dados falsos ✓ Corrupção de dados ✓ Interceptação de informação ✓ Desvio de informação ✓ Uso de programas ou códigos maliciosos ✓ Sabotagens ✓ Invasão de sistemas ✓ Acessos não autorizados a sistemas	✓ Controle de acessos físicos e lógicos ✓ Compartilhamento de conhecimento.
	Inexistência de Políticas e Normas de controle para o uso	Fraude	✓ Apropriações indevidas ✓ Corrupção e informações falsas	✓ Condução de programa para Gestão de Segurança da Informação e Comunicações

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
	correto dos ativos de informação		✓ Interceptação de informação ✓ Desvio de informação ✓ Invasão de sistema ✓ Obtenção de vantagens indevidas	
	Inexistência de controle de acesso físico	Arrombamento	✓ Roubo ✓ Acessos indevidos ✓ Vazamento de informação ✓ Má utilização dos recursos de TI ✓ Indisponibilidades dos serviços de TI	✓ Utilização de biometria digital na sala segura da CGTI ✓ Sistema de câmera de segurança ✓ Controle de acesso físico (recepção setorial) ✓ Uso de crachá
	Ambiente de telefonia desatualizado ou sem mecanismos de segurança adequados	Escuta telefônica	✓ Interceptação de dados	✓ Condução de processo licitatório para renovação contratual e atualização do ambiente ✓ Utilização do protocolo TLS
INFRAESTRUTURA	Manutenção insuficiente ou instalação defeituosa de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	✓ Perda de informação ✓ Indisponibilidade de serviço	✓ Rotina de contingência
	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia	✓ Recursos desatualizados ✓ Perda de dados ✓ Má utilização dos recursos de TI	✓ Rotina de contingência
	Sensibilidade à umidade, poeira ou sujeira	Poeira, corrosão, congelamento	✓ Defeitos de hardware ✓ Lentidão dos serviços ✓ Aquecimento de equipamentos ✓ Indisponibilidade de serviço ✓ Perda de garantia	✓ Limpeza local ✓ Climatização

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
	Sensibilidade à radiação eletromagnética	Radiação eletromagnética	✓ Defeitos de hardware e mídia ✓ Perda de dados	✓ Utilização de cabo blindado ✓ Atendimento ao padrão de cabeamento estruturado
	Inexistência de um controle de mudanças de configuração	Erro durante o uso	✓ Perda de dados ✓ Recursos desatualizados ✓ Má administração dos recursos de TI	-
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia	✓ Inoperabilidade dos recursos de TI ✓ Queima de equipamento ✓ Perda de dados	✓ Utilização de nobreak ✓ Utilização de gerador
	Sensibilidade a variações de temperatura	Fenômeno meteorológico	✓ Defeitos de hardware ✓ Perda de dados ✓ Variações de desempenho ✓ Queima de equipamento	✓ Utilização de Para raio ✓ Rede elétrica estabilizada
	Armazenamento não protegido	Furto de mídia ou documentos	✓ Acessos indevidos ✓ Vazamento de informação ✓ Má utilização dos recursos de TI ✓ Indisponibilidades dos serviços de TI	✓ Utilização de cofre ✓ Utilização de biometria digital na sala segura da CGTI
	Descuidado durante o descarte	Furto de mídia ou documentos	✓ Acessos indevidos ✓ Vazamento de informação ✓ Má utilização dos recursos de TI	✓ Utilização de triturador de papel e mídia
	Utilização de cópias não controladas	Furto de mídias ou documentos	✓ Acessos indevidos ✓ Vazamento de informação ✓ Má utilização dos recursos de TI ✓ Má administração dos recursos de TI	-

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
	Inexistência de mecanismos de autenticação e identificação	Forjamento de direitos	✓ Acessos indevidos ✓ Vazamento de informação ✓ Perda de disponibilidade, integridade, confidencialidade e autenticidade	✓ Controle de acesso lógico (login/senha) ✓ Uso de crachá
	Tabelas de senhas desprotegidas	Forjamento de direitos	✓ Acessos indevidos ✓ Vazamento de informação ✓ Perda de disponibilidade, integridade, confidencialidade e autenticidade	-
	Gerenciamento mal feito de senhas	Forjamento de direitos	✓ Acessos indevidos ✓ Vazamento de informação ✓ Perda de disponibilidade, integridade, confidencialidade e autenticidade	✓ Utilização do Active Directory - AD
	Serviços desnecessários habilitados	Processamento ilegal de dados	✓ Acessos indevidos ✓ Vazamento de informação ✓ Indisponibilidades dos serviços de TI ✓ Consumo excessivo de link e processador	✓ Utilização de – Group Policy -GPO
	Software novo ou imaturo	Defeito de *software*	✓ Falha no software ✓ Inconsistência de dados ✓ Comprometimento dos serviços de rede	✓ Utilização de ambiente de homologação
	Especificações confusas ou incompletas para os desenvolvedores	Defeito de *software*	✓ Falha no software ✓ Inconsistência de dados ✓ Comprometimento dos serviços de rede ✓ Não atendimento a finalidade do software	✓ Levantamento de requisitos ✓ Definição de escopo ✓ Utilização de metodologia

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
	Inexistência de um controle eficaz de mudança	Defeito de *software*	✓ Falha no software ✓ Inconsistência de dados ✓ Perda de dados ✓ Recursos desatualizados ✓ Má administração dos recursos de TI	-
	Download e uso não controlado de *software*	Alteração do *software*	✓ Falha no software ✓ Inconsistência de dados ✓ Perda de dados ✓ Má administração dos recursos de TI	✓ Firewall
	Inexistência de cópias de segurança	Alteração do *software*	✓ Inconsistência de dados ✓ Perda de dados ✓ Má administração dos recursos de TI	✓ Utilização de solução de backup
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos	✓ Roubo ✓ Acessos indevidos ✓ Perda de dados ✓ Vazamento de informação ✓ Indisponibilidades dos serviços de TI	✓ Utilização de biometria digital na sala segura da CGTI ✓ Sistema de câmera de segurança ✓ Controle de acesso físico (recepção setorial) ✓ Uso de crachá
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento	✓ Má administração dos recursos de TI ✓ Acesso indevido ✓ Vazamento de informação ✓ Indisponibilidades dos serviços de TI	✓ Utilização de aplicativo de gerenciamento (SCCM)
	Inexistência de evidências que comprovem o envio ou recebimento de mensagens	Repúdio de ações	✓ Má administração dos recursos de TI ✓ Acesso indevido ✓ Vazamento de informação	✓ Utilização de funcionalidades do Microsoft Exchange e Active Directory – AD

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
			✓ Perda de integridade, confidencialidade e autenticidade	
	Junções de cabeamento mal feitas	Erro durante o uso	✓ Falha de comunicação ✓ Má administração dos recursos de TI ✓ Indisponibilidades dos serviços de TI ✓ Perda de disponibilidade	✓ Acompanhamento por técnico especializado do MTur ✓ Utilização de cabo blindado ✓ Atendimento ao padrão de cabeamento estruturado
	Gerenciamento de rede inadequado, quanto à configuração de roteamentos	Saturação do sistema de informação	✓ Falha de comunicação ✓ Má administração dos recursos de TI ✓ Indisponibilidades dos serviços de TI ✓ Sobrecarga no tráfego de rede	✓ Utilização das recomendações de cada fabricante ✓ Realização de configurações de acordo com a necessidade do órgão
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento	✓ Má administração dos recursos de TI ✓ Indisponibilidades dos serviços de TI ✓ Acesso indevido ✓ Vazamento de informação ✓ Sobrecarga no tráfego de rede ✓ Programas maliciosos ✓ Danificação de equipamento	✓ Antivírus ✓ Firewall
	Uso inadequado de mecanismos de controle de acesso físico a locais sensíveis	Destruição de equipamento ou mídia	✓ Roubo ✓ Acessos indevidos ✓ Perda de dados ✓ Vazamento de informação ✓ Danificação de equipamento	✓ Utilização de biometria digital na sala segura da CGTI ✓ Sistema de câmera de segurança ✓ Controle de acesso físico (recepção setorial)

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
			✓ Indisponibilidades dos serviços de TI	✓ Uso de crachá
	Localização em área suscetível a inundações	Inundação	✓ Indisponibilidades dos serviços de TI ✓ Perda de equipamentos e dados	-
	Falta de Contingência	Comprometimento dos dados	✓ Má administração dos recursos de TI ✓ Indisponibilidades dos serviços de TI ✓ Sobrecarga no tráfego de rede ✓ Inoperabilidade de software ✓ Perda da disponibilidade	-
	Firewall desatualizado	Uso não autorizado de equipamento	✓ Má administração dos recursos de TI ✓ Indisponibilidades dos serviços de TI ✓ Sobrecarga no tráfego de rede ✓ Inoperabilidade de software ✓ Programas maliciosos ✓ Acessos indevidos ✓ Vazamento de informação ✓ Perda de dados	✓ Condução de processo licitatório para renovação contratual e atualização do ambiente
APLICAÇÕES	Inexistência de procedimentos de teste de *softwares*.	Abuso de direitos	✓ Falha no software ✓ Comprometimento dos serviços de rede	✓ Utilização de ambiente de homologação
	Falhas conhecidas no *software*	Abuso de direitos	✓ Comprometimento da integridade das informações ✓ Falha no software	-

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
			✓ Comprometimento dos serviços de rede ✓ Falha no acompanhamento e desenvolvimento do software	
	Não execução do "*logout*" ao se deixar uma estação de trabalho	Abuso de direitos	✓ Acessos indevidos ✓ Comprometimento da integridade das informações ✓ Vazamento de informações	✓ Compartilhamento de conhecimento ✓ Conscientização individual
	Atribuição errônea de direitos de acesso	Abuso de direitos	✓ Acessos indevidos ✓ Vazamento de informação ✓ Perda de disponibilidade, integridade, confidencialidade e autenticidade das informações	-
	Interface de usuário complexa	Erro durante uso	✓ Dificuldade no uso do software ✓ Má utilização dos recursos ✓ Falhas e comprometimento das informações ✓ Desuso do software	-
	Inexistência de documentação	Erro durante uso	✓ Inoperabilidade do *software* ✓ Falhas e comprometimento dos serviços de rede	✓ Utilização de metodologia
	Parâmetros Incorretos	Erro durante uso	✓ Falha no software ✓ Falha no acompanhamento e desenvolvimento do software ✓ Perda de integridade	✓ Levantamento de requisitos ✓ Definição de escopo ✓ Utilização de metodologia
	Datas incorretas	Erro durante uso	✓ Falha no software ✓ Falha no acompanhamento e desenvolvimento do software ✓ Perda de integridade	✓ Levantamento de requisitos ✓ Definição de escopo ✓ Utilização de metodologia

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
SERVIÇOS	Inexistência de um procedimento formal para o registro de remoção de usuários	Abuso de direitos	✓ Acesso indevido ✓ Controle de acesso desatualizado ✓ Vazamento de informação	✓ Solicitações feitas via memorando ou e-mail ✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações
	Inexistência de processo formal para a análise crítica dos direitos de acesso	Abuso de direitos	✓ Acesso indevido ✓ Vazamento de informação ✓ Má administração de controle de acesso	✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações
	Provisões de segurança insuficientes ou inexistentes em contratos com clientes e/ou terceiros	Abuso de direitos	✓ Acesso indevido ✓ Vazamento de informação ✓ Má administração de contratos de TI	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI
	Inexistência de procedimentos de monitoramento das instalações de processamento de informações	Abuso de direitos	✓ Acesso indevido ✓ Vazamento de informação ✓ Má administração dos recursos de TI ✓ Falhas e comprometimento dos serviços de rede	✓ Realização do mapeamento dos processos de Infraestrutura/CGTI
	Inexistência de auditorias periódicas	Abuso de direitos	✓ Falha no acompanhamento e controle dos serviços de TI	-

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
	Inexistência de procedimentos para a identificação e análise/avaliação de riscos	Abuso de direitos	✓ Falha no gerenciamento de riscos de TI	✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Instituição da Política de Segurança da Informação e Comunicações ✓ Condução de projeto para elaboração do Plano Diretor de SIC ✓ Realização do mapeamento dos processos de análise/avaliação de risco de acordo com as Normas Complementares do GSI/PR e Guia de Referência para a Segurança de Infraestruturas Críticas da Informação
	Acordo de nível de serviço (SLA) inexistente ou ineficaz	Violação das condições de uso do sistema de informação	✓ Inoperabilidade dos serviços de TI ✓ Dificuldade na aplicação de multas e sanções	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI (MPOG) ✓ Utilização de aplicativo de monitoramento (ZABBIX
	Procedimento e controle de sistemas de gerenciamento de segurança inexistentes	Comprometimento dos dados	✓ Acesso indevido ✓ Vazamento de informação ✓ Falhas e comprometimento dos serviços de rede ✓ Inoperabilidade do software ✓ Perda de disponibilidade, integridade, confidencialidade e autenticidade	✓ Utilização de aplicativo de gerenciamento (SCCM)
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de ações	✓ Falha no gerenciamento de recursos humanos ✓ Não comprometimento da equipe de trabalho	✓ Instituição do Comitê de SIC ✓ Instituição do Gestor de SIC ✓ Instituição do Grupo de Trabalho de SIC ✓ Núcleo de SIC da CGTI

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
			✓ Ineficiência na execução das atividades de segurança	✓ Instituição da Política de Segurança da Informação e Comunicações
	Plano de continuidade de serviços inexistente	Falha nos serviços	✓ Má administração dos recursos de TI ✓ Indisponibilidades dos serviços de TI ✓ Sobrecarga no tráfego de rede ✓ Inoperabilidade de software ✓ Perda da disponibilidade ✓ Perda de dados	-
	Política de uso de e-mail inexistente	Erro durante o uso	✓ Acesso indevido ✓ Vazamento de informação ✓ Perda de integridade, confidencialidade e autenticidade ✓ Corrupção e informações falsas ✓ Programas maliciosos ✓ Sobrecarga no tráfego de rede ✓ SPAM	✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação
	Ausência de registros de auditoria (*logs*)	Erro durante o uso	✓ Falha no acompanhamento e controle dos serviços de TI	-
	Processo disciplinar no caso de incidentes de segurança inexistente	Furto de equipamentos ou dados	✓ Falha no gerenciamento e controle de recursos humanos ✓ Perda de dados ✓ Vazamento de informação ✓ Extravio de equipamento e componentes	✓ Definição de iniciativa para criação da Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais do MTur e seu respectivo plano de gerenciamento, no Planejamento Estratégico 2013

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

CATEGORIA DOS ATIVOS DE INFORMAÇÃO	VULNERABILIDADE	AMEAÇAS	CONSEQUÊNCIAS	AÇÕES ADOTADAS (CONTROLES)
			✓ Indisponibilidades dos serviços de TI	
	Política de uso de recursos de informática inexistente	Furto de equipamentos ou dados	✓ Apropriações indevidas ✓ Corrupção e informações falsas ✓ Interceptação de informação ✓ Desvio de informação ✓ Invasão de sistema	✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Instituição da Política de Segurança da Informação e Comunicações
	Inexistência de controle de ativos fora da organização	Furto de equipamentos ou dados	✓ Acesso indevido ✓ Perda de dados ✓ Comprometimento de dados ✓ Extravio de equipamento e componentes ✓ Má administração dos recursos de TI	✓ Utilização de formulário para entrada/saída de ativos com assinatura dos respectivos responsáveis ✓ Conferência patrimonial de entrada/saída de equipamento
	Inexistência de procedimentos de direitos de propriedade intelectual	Uso de cópias de aplicativos falsificadas ou ilegais.	✓ Exposição a vírus de software ✓ Corrupção de disco ✓ Defeito no software ✓ Crime de violação dos direitos autorais ✓ Má utilização dos recursos de TI	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI ✓ Licenças de uso de software

Tabela 8 – Vulnerabilidades x Ameaças x Consequências x Ações de SIC adotadas

3.4 Estimativa dos Riscos Levantados

A Estimativa dos Riscos é um processo utilizado para atribuir valores à probabilidade e consequências de um risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade - DICA nos Ativos de Informação. Na qual, é realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio. O MTur designou os valores qualitativos para a estimativa dos riscos, probabilidade e impactos dos riscos identificados neste PDSIC. As Tabelas 9, 10 e 11 determinam a escala de medida a ser usada e os critérios que permitam posicionar um ativo no seu correto lugar nessa escala, em função de seu valor qualitativo:

3.4.1 Valor

Primeiramente, um valor é designado para cada ativo. Esse valor refere-se às possíveis consequências adversas que podem surgir quando o ativo é ameaçado. O valor (do ativo) é definido para cada ameaça aplicável ao ativo:

ESTIMATIVAS DOS RISCOS	VALOR
Muito baixo	1
Baixo	2
Médio	3
Alto	4
Muito alto	5

Tabela 9 – Valor do Ativo

3.4.2 Probabilidade

Para a Gestão de Risco referir-se à chance de algo acontecer, não importando se de forma definida, medida ou determinada ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (tal como probabilidade ou frequência durante um determina do período de tempo):

PROBABILIDADE	VALOR
Muito baixo	1
Baixo	2
Médio	3
Alto	4
Muito alto	5

Tabela 10 – Probabilidade

3.4.3 Impactos

Os impactos são resultados indesejados da ocorrência de uma ameaça contra um bem, que resulta em perda mensurável para uma organização. Quase todo risco tem um impacto, embora de difícil previsão:

IMPACTO	DESCRIÇÃO
Muito baixo	Não existe impacto financeiro ou impacto significativo sobre a estratégia ou atividades operacionais.
Baixo	Impacto baixo sobre a estratégia ou atividades operacionais.
Médio	Impacto alto sobre a estratégia ou atividades operacionais da organização.
Alto	Impacto significativo sobre a estratégia ou atividades operacionais da organização.
Muito alto	Evento catastrófico com grande impacto sobre a estratégia ou atividades operacionais da organização.

Tabela 11 – Impacto

3.4.4 Riscos identificados

Os riscos de operação dos serviços de TI estão diretamente relacionados às operações de negócios, e a mitigação destes riscos é fator crítico na gestão corporativa e de TI. Gerenciar os riscos de TI e de Segurança da Informação significa reconhecer as vulnerabilidades e ameaças do ambiente, avaliá-las e propor controles (soluções e ferramentas) que mitiguem os riscos aos níveis aceitáveis.

A Tabela 12 descreve a estimativa dos riscos levantados e determina a escala de medida a ser usada e os critérios que permitam posicionar um ativo no seu correto lugar nessa escala, em função de seu valor qualitativo

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	PROBALIDADE	IMPACTO	ESTIMATIVA DO NIVEL DE RISCO	VALOR
Abuso dos recursos computacionais	MUITO ALTO	ALTO	MUITO ALTO	4
Acesso indevido (lógico)	BAIXO	MUITO ALTO	MEDIO	3
Acesso indevido (físico)	MEDIO	ALTO	MEDIO	3
Agressão a funcionário	MUITO BAIXO	BAIXO	BAIXO	2
Apropriações indevidas	BAIXO	ALTO	BAIXO	2
Aquecimento de equipamentos	BAIXO	MUITO ALTO	MEDIO	3
Ataques a sistemas	BAIXO	MUITO ALTO	MEDIO	3
Ataques com bombas	MUITO BAIXO	MUITO ALTO	BAIXO	2
Atividades executadas inadequadamente por falta de pessoal	MEDIA	ALTO	MEDIO	3
Chantagem	MUITO BAIXO	ALTO	BAIXO	2
Controle de acesso desatualizado	MUITO ALTO	MUITO ALTO	MUITO ALTO	5
Corrupção de dados	MUITO ALTO	MUITO ALTO	MUITO ALTO	5
Crime de violação dos direitos autorais	MUITO BAIXO	ALTO	BAIXO	2
Danificação de equipamento	MUITO ALTO	ALTO	ALTO	4
Defeitos de hardware	MEDIO	ALTO	MEDIO	3
Defeito no software	MEDIO	MEDIO	MEDIO	3
Desuso do software	MEDIO	MEDIO	MEDIO	3
Dificuldade na aplicação de multas e sanções	BAIXO	MUITO ALTO	MEDIO	3
Dificuldade no uso do software	MEDIO	ALTO	MEDIO	3
Engenharia social	MEDIO	MUITO ALTO	ALTO	4
Exploração econômica	BAIXO	ALTO	MEDIO	3
Falha de comunicação	MUITO BAIXO	MUITO ALTO	BAIXO	2

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	PROBALIDADE	IMPACTO	ESTIMATIVA DO NIVEL DE RISCO	VALOR
Inexistência de registro de auditoria (monitoramento)	ALTO	ALTO	ALTO	4
Falha no acompanhamento e desenvolvimento do software	BAIXO	MUITO ALTO	MEDIO	3
Falha no gerenciamento de recursos humanos	MUITO BAIXO	ALTO	BAIXO	2
Falha no gerenciamento de riscos de TI	BAIXO	MUITO ALTO	MEDIO	3
Falta de qualificação profissional	MEDIO	MEDIO	MEDIO	3
Fraudes	BAIXO	MUITO ALTO	MEDIO	3
Garantir uma vantagem política	MUITO BAIXO	MUITO ALTO	BAIXO	2
Guerra de informação	MUITO BAIXO	MUITO ALTO	BAIXO	2
Inconsistência de dados	BAIXO	MUITO ALTO	MEDIO	3
Indisponibilidades dos serviços de TI	MEDIA	MUITO ALTO	ALTO	4
Ineficiência na execução das atividades de segurança	BAIXO	ALTO	MEDIO	3
Inoperabilidade do software	BAIXO	ALTO	MEDIO	3
Instalações e remoções indevidas	ALTO	ALTO	ALTO	4
Interceptação de informação	BAIXO	ALTO	MEDIO	3
Invasão de privacidade	MÉDIO	ALTO	MEDIO	3
Invasão de sistemas	BAIXO	ALTO	MEDIO	3
Lentidão dos serviços	MEDIO	MEDIO	MEDIO	3
Má administração de contratos de TI	MUITO BAIXO	MUITO ALTO	MUITO ALTO	5
Má administração de controle de acesso	ALTO	MUITO ALTO	ALTO	4
Má administração dos recursos de TI	BAIXO	MUITO ALTO	MEDIO	3
Não atendimento a finalidade do software	MEDIO	ALTO	MEDIO	3
Não comprometimento da equipe de trabalho de segurança da informação	MUITO BAIXO	MUITO ALTO	BAIXO	2

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	PROBALIDADE	IMPACTO	ESTIMATIVA DO NIVEL DE RISCO	VALOR
Negação de serviço	MUITO BAIXO	MUITO ALTO	BAIXO	2
Obtenção de vantagens indevidas	BAIXO	MUITO ALTO	MEDIO	3
Perda de dados	ALTO	MUITO ALTO	ALTO	4
Perda de disponibilidade	BAIXO	MUITO ALTO	MEDIO	3
Perda de integridade	BAIXO	MUITO ALTO	MEDIO	3
Perda de confidencialidade	MEDIO	MUITO ALTO	ALTO	4
Perda de autenticidade	BAIXO	MUITO ALTO	MEDIO	3
Perda de garantia	BAIXO	MUITO ALTO	MEDIO	3
Pichação de sites	MUITO BAIXO	MUITO ALTO	BAIXO	2
Profissionais com perfis inadequados para as atividades da área	MEDIO	ALTO	MEDIO	3
Queima de equipamento	MUITO BAIXO	MUITO ALTO	BAIXO	2

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	PROBALIDADE	IMPACTO	ESTIMATIVA DO NIVEL DE RISCO	VALOR
Recursos desatualizados	BAIXO	MEDIO	BAIXO	2
Roubo/furto	BAIXO	ALTO	MEDIO	3
Sabotagens	MUITO BAIXO	MUITO ALTO	BAIXO	2
Sobrecarga de link internet	MEDIO	ALTO	MEDIO	3
Sobrecarga de trabalho	ALTO	ALTO	ALTO	4
Sobrecarga no tráfego de rede	BAIXO	MUITO ALTO	MEDIO	3
Spam	MEDIO	MEDIO	MEDIO	3
Uso de programas ou códigos maliciosos	BAIXO	MUITO ALTO	MEDIO	3
Uso inadequado dos ativos de informação	MEDIO	MEDIO	MEDIO	3
Variações de desempenho de equipamento	MUITO BAIXO	MEDIO	BAIXO	2
Vazamento de informação	MUITO ALTO	MUITO ALTO	MUITO ALTO	5

Tabela 12 – Estimativa dos Riscos

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

A Figura 4 apresenta a consolidação da estimativa dos riscos levantados e possibilita uma visão geral da situação de Segurança da Informação e Comunicações na Coordenação-Geral de Tecnologia da Informação do MTur:

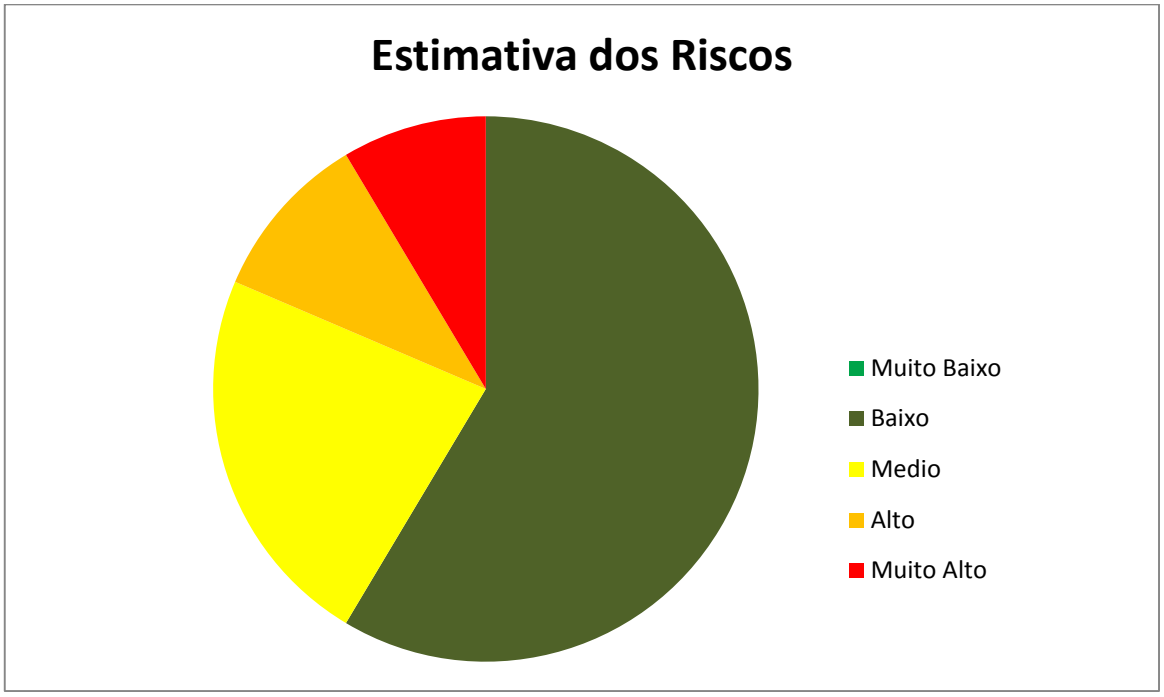

Figura 4 - Visão Geral - Estimativa dos Riscos

Já a Figura 5 apresenta a consolidação da estimativa dos riscos levantados e possibilita uma visão detalhada da estimativa dos riscos identificados na Coordenação-Geral de Tecnologia da Informação do MTur:

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

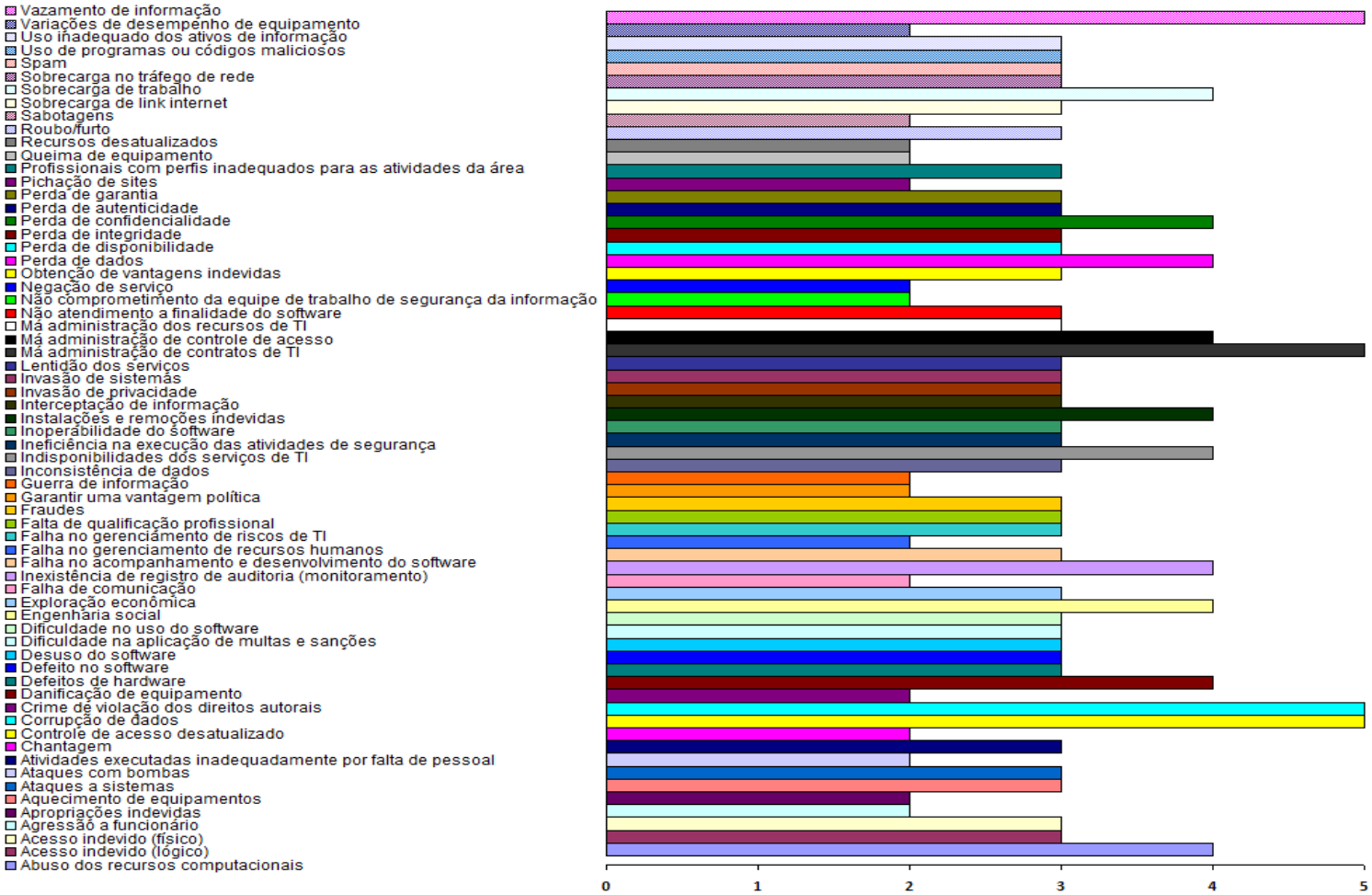

Figura 5 - Visão Detalhada - Estimativa dos Riscos

3.5 Avaliação dos Riscos

A avaliação de Riscos de TI e Segurança da Informação são baseadas na elaboração da uma matriz de risco estruturada, que identifica os principais itens que compõe o ambiente avaliado, especificando com clareza suas vulnerabilidades e ameaças. Além disso, a matriz apresenta o impacto da exploração destas vulnerabilidades pelas ameaças e a probabilidade desta ocorrência.

Os riscos identificados possuem um atributo chamado de Exposição do Risco. A Exposição do Risco então é resultado da função Impacto x Probabilidade e é estimado tanto quantitativamente (estimativa numérica) como qualitativamente (estimativa conceitual). O resultado dessa operação possui valores possíveis de 1 a 25. Dessa forma os riscos se enquadram de acordo com a matriz apresentada na Figura 6:

Probabilidade					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
					Impacto

Figura 6 - Matriz de risco

A escala acima pode ser aproximada, mais genericamente, para:

Muito baixo: 1 a 3

Baixo: 4 a 7

Médio: 8 a 14

Alto: 15 a 20

Muito alto: 21 a 25

De posse da matriz de risco é possível especificar as ações necessárias para a mitigação dos mesmos, seguindo a priorização qualitativa.

3.5.1 Riscos Aceitáveis

A Norma Complementar Nº 04/IN01/DSIC/GSIPR apresenta uma abordagem sistemática do processo Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, com o objetivo de manter os riscos em níveis aceitáveis. Na etapa de aceitação dos riscos são verificados os resultados do processo executado, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.

3.5.2 Riscos Tratáveis

Dando continuidade à etapa de avaliação dos riscos, para este PDSIC, foram relacionados os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pelo MTur.

3.5.2.1Ações de Tratamento

As ações de tratamento foram identificadas, assim como na Identificação dos Riscos, em reuniões de *brainstorm* com os membros do Núcleo de SIC e equipe de TI do Ministério do Turismo.

Para cada risco identificado na etapa anterior, foram definidos os aceitáveis e os que requerem tratamento e, em seguida definidas as ações de tratamento necessárias, conforme demonstra a Tabela 13:

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
Abuso dos recursos computacionais	MUITO ALTO		X	✓ Definição de Normas de SIC ✓ Cultura e conscientiza de SIC
Acesso indevido (lógico)	MÉDIO		X	✓ Definição de Norma de controle de acesso logico e de SIC ✓ Cultura e conscientização de SIC
Acesso indevido (físico)	MEDIO		X	✓ Definição de Norma de SIC ✓ Cultura e conscientização de SIC ✓ Uso de crachá de identificação
Agressão a funcionário	BAIXO	X		-
Apropriações indevidas	BAIXO	X		-
Aquecimento de equipamentos	MEDIO		X	✓ Manutenção de sistema de climatização ✓ Manutenção periódica dos equipamentos ✓ Distribuição física adequada para os equipamentos
Ataques a sistemas	MEDIO		X	✓ Utilização de firewall ✓ Controle de acesso lógico
Ataques com bombas	BAIXO	X		-
Atividades executadas inadequadamente por falta de pessoal	MEDIO		X	✓ Condução de projeto para elaboração da proposta de criação de cargos de ATI's do MTur, para solicitação ao MPOG
Chantagem	BAIXO	X		-
Controle de acesso desatualizado	MUITO ALTO		X	✓ Antivírus ✓ Firewall ✓ Atualização periódica dos aplicativos ✓ Atualização e manutenção dos controles de acesso de acordo com as informações repassadas pelos titulares das unidades administrativas, COGEP, CGRL à CGTI
Corrupção de dados	MUITO ALTO		X	✓ Condução de programa para Gestão de Segurança da Informação e Comunicações. ✓ Controle de acessos físicos e lógicos ✓ Cultura e conscientização de SIC
Crime de violação dos direitos autorais	BAIXO	X		-
Danificação de equipamento	ALTO		X	✓ Manutenção periódica dos equipamentos ✓ Cultura e conscientização de SIC

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
				✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à Tecnologia da Informação ✓ Instituição da Política de Segurança da Informação e Comunicações
Defeitos de *hardware*	MEDIO		X	✓ Atualização e manutenção periódica dos equipamentos
Defeito no *software*	MEDIO		X	✓ Levantamento de requisitos ✓ Definição de escopo ✓ Utilização de metodologia ✓ Ambiente de homologação
Desuso do *software*	MEDIO	X		-
Dificuldade na aplicação de multas e sanções	MEDIO		X	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI (MPOG)
Dificuldade no uso do *software*	MEDIO		X	✓ Cultura e conscientização de SIC ✓ Condução de projeto para elaboração de Plano de Capacitação ✓ Compartilhamento de conhecimento
Engenharia social	ALTO		X	✓ Cultura e conscientização de SIC ✓ Instituição da Política de Segurança da Informação e Comunicações
Exploração econômica	MEDIO		X	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI (MPOG) ✓ Instituição da Política de Segurança da Informação e Comunicações
Falha de comunicação	BAIXO		X	✓ Utilização de cabo blindado ✓ Atendimento ao padrão de cabeamento estruturado. ✓ Gerenciamento e monitoramento da rede.
Inexistência de registro de auditoria (monitoramento)	ALTO		X	✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Analise e avaliação dos riscos de TI
Falha no acompanhamento e desenvolvimento do *software*	MEDIO		X	✓ Levantamento de requisitos ✓ Definição de escopo ✓ Utilização de metodologia ✓ Ambiente de homologação

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
Falha no gerenciamento de recursos humanos	BAIXO		X	✓ Redistribuição de atividades de acordo com perfil profissional existente
Falha no gerenciamento de riscos de TI	MEDIO		X	✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Analise e avaliação dos riscos de TI ✓ Mapeamento do processo de Gestão de Risco ✓ Criação da ETIR
Falta de qualificação profissional	MEDIO		X	✓ Condução de projeto para elaboração de Plano de Capacitação
Fraudes	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Utilização de aplicação MTurDoc ✓ Condução de processo para contratação de solução GED
Garantir uma vantagem política	BAIXO	X		-
Guerra de informação	BAIXO	X		-
Inconsistência de dados	MEDIO		X	✓ Utilização de ambiente de homologação ✓ Gerenciamento do Banco de Dados ✓ Gerenciamento da rede
Indisponibilidades dos serviços de TI	ALTO		X	✓ Gerenciamento da rede ✓ Redundância de links ✓ Site de contingencia ✓ Sala Segura
Ineficiência na execução das atividades de segurança	MEDIO		X	✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Instituição da Política de Segurança da Informação e Comunicações ✓ Cultura e conscientização de SIC ✓ Condução de projeto para elaboração de Plano de Capacitação ✓ Instituição do Grupo de Trabalho de SIC
Inoperabilidade do software	MEDIO		X	✓ Site de contingencia. ✓ Utilização de metodologia.

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
				✓ Firewall.
Instalações e remoções indevidas	ALTO		X	✓ Controle de acessos físicos e lógicos ✓ Utilização de metodologia ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Instituição da Política de Segurança da Informação e Comunicações ✓ Cultura e conscientização de SIC
Interceptação de informação	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Invasão de privacidade	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Invasão de sistemas	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Lentidão dos serviços	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Má administração de contratos de TI	MUITO ALTO		X	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI (MPOG) ✓ Utilização de aplicativo de monitoramento
Má administração de controle de acesso	ALTO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
Má administração dos recursos de TI	MEDIO		X	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI (MPOG) ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ PEI, PETI,PDTI, PMA, PDSIC
Não atendimento a finalidade do software	MEDIO		X	✓ Levantamento de requisitos ✓ Definição de escopo ✓ Utilização de metodologia
Não comprometimento da equipe de trabalho de segurança da informação	BAIXO		X	✓ Cultura e conscientização de SIC ✓ Condução de projeto para elaboração de Plano de Capacitação ✓ Instituição do Grupo de Trabalho de SIC ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações
Negação de serviço	BAIXO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Obtenção de vantagens indevidas	MEDIO	X		✓
Perda de dados	ALTO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Perda de disponibilidade	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Cultura e conscientização de SIC ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Instituição da Política de Segurança da Informação e Comunicações
Perda de integridade	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
				✓ Cultura e conscientização de SIC ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Instituição da Política de Segurança da Informação e Comunicações
Perda de confidencialidade	ALTO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Cultura e conscientização de SIC ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Instituição da Política de Segurança da Informação e Comunicações
Perda de autenticidade	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Cultura e conscientização de SIC ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Instituição da Política de Segurança da Informação e Comunicações
Perda de garantia	MEDIO		X	✓ Utilização da IN04/2010 para o processo de contratação de recursos de TI (MPOG) ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Pichação de *sites*	BAIXO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Utilização de metodologia
Profissionais com perfis inadequados para as atividades da área	MEDIO		X	✓ Condução de projeto para elaboração de Plano de Capacitação ✓ Redistribuição de atividades de acordo com perfil profissional existente

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
Queima de equipamento	BAIXO		X	✓ Manutenção periódica. ✓ Instalações de rede estabilizadas ✓ Cultura e conscientização de SIC
Recursos desatualizados	BAIXO		X	✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Atualização do parque computacional
Roubo/furto	MEDIO		X	✓ Utilização de biometria digital na sala segura da CGTI ✓ Sistema de câmera de segurança ✓ Controle de acesso físico (recepção setorial) ✓ Uso de crachá
Sabotagens	BAIXO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Cultura e conscientização de SIC ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações
Sobrecarga de link internet	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Cultura e conscientização de SIC
Sobrecarga de trabalho	ALTO		X	✓ Condução de projeto para elaboração da proposta de criação de cargos de ATI's do MTur, para solicitação ao MPOG
Sobrecarga no tráfego de rede	MEDIO		X	✓ Controle de acessos físicos e lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Cultura e conscientização de SIC
Spam	MEDIO		X	✓ Controle de acessos lógicos ✓ Firewall ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento ✓ Cultura e conscientização de SIC
Uso de programas ou códigos maliciosos	MEDIO		X	✓ Antivírus ✓ Firewall ✓ Cultura e conscientização de SIC

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

RISCOS	ESTIMATIVA DO NIVEL DE RISCO	RISCOS ACEITÁVEIS	RISCOS TRATÁVEIS	ACOES DE TRATAMENTO
				✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Instituição da Política de Segurança da Informação e Comunicações
Uso inadequado dos ativos de informação	MEDIO		X	✓ Cultura e conscientização de SIC ✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Instituição da Política de Segurança da Informação e Comunicações ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento
Variações de desempenho de equipamento	BAIXO		X	✓ Manutenção periódica ✓ Instalações de rede estabilizadas ✓ Cultura e conscientização de SIC
Vazamento de informação	MUITO ALTO		X	✓ Cultura e conscientização de SIC ✓ Publicação da Instrução Normativa Nº 04, de 30 de junho de 2010 que disciplina procedimentos operacionais e de segurança da informação relativos à tecnologia da informação ✓ Instituição da Política de Segurança da Informação e Comunicações ✓ Condução de programa para Gestão de Segurança da Informação e Comunicações ✓ Controle de acessos físicos e lógicos ✓ Gerenciamento da rede ✓ Aplicativos de monitoramento

Tabela 13 – Avaliação dos Riscos

4 Planejamento

A Norma Complementar Nº 11/IN01/DSIC/GSIPR, de 30 de janeiro de 2010, estabelece as diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

Segundo a NC 11 a "*avaliação de conformidade em SIC pode ser subsidiada por meio da análise e avaliação de riscos e auditorias internas previsto no item 3.3.5 da NC 02/IN01/GSIPR/DSIC*", na qual cita que o órgão deverá "*conduzir auditoria interna, também denominada auditoria de primeira parte, das ações de segurança da informação e comunicações a intervalos planejados de pelo menos uma vez ao ano*".

Com base nos dados e informações descritas no capítulo "Situação Atual", e adotando uma abordagem que viabilize ao MTur definir, implementar e manter níveis adequados de Segurança da Informação, bem como prever a continuidade após a execução deste Plano Diretor, através de regras e processos formalizados e amplamente divulgados a toda instituição, o Ministério do Turismo desenvolveu este PDSIC como um plano de ação para a implementação de projetos de SIC para os próximos três anos, com o objetivo de ser um instrumento de orientação e priorização, buscando a evolução do nível de Segurança da Informação e Comunicações. Dentre os selecionados, alguns servirão para manutenção e acompanhamento dos projetos já desenvolvidos, com isso eles terão sua atualização garantida.

4.1 Elaboração de *Checklist* para verificação de Conformidade com a Norma ABNT NBR ISO/IEC 27002

O conceito de Segurança da Informação está relacionado à adoção de políticas e ações que visam preservar o valor que as informações possuem para um indivíduo ou uma organização. Essas políticas para garantir a Segurança da Informação englobam os atributos de confidencialidade, integridade, disponibilidade e autenticidade.

A elaboração do *checklist* tem como propósito disponibilizar uma base de conhecimento tendo como referências as normas de segurança, com o propósito de monitorar a conformidade e a efetividade através de auditorias de conformidade, fornecendo informações gerenciais a estrutura de Gestão da Segurança da Informação do Ministério do Turismo.

Considerando estas características e o aspecto sistêmico e organizacional relacionado à cultura de Segurança da Informação crítico para a Gestão de Segurança da Informação, observa-se que o *checklist* constitui-se como uma técnica de pesquisa adequada para estudos relativos à situação destes processos de gestão em organizações. Com isso, podem ser feitas análises com diversas abordagens: verificação de conformidade, governança, nível de gestão, qualidade e resultados.

A Tabela 14 demonstra o resultado da pesquisa realizada:

TEMAS	PERGUNTAS	SIM	NÃO	OBSERVAÇÕES
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - POSIC	Há uma Política de Segurança da Informação aprovada pela alta administração, publicada e comunicada?	X		
	Há um responsável pela Gestão da Política de Segurança da Informação?	X		
	São realizadas análises críticas/revisões da Política de Segurança da Informação a intervalos planejados e quando ocorrem mudanças significativas?	X		POSIC/2013 Atualização até 3 anos ou sempre que necessário
SEGURANÇA ORGANIZACIONAL	Há infraestrutura de Segurança da Informação para gerenciar as ações corporativas?	X		Comitê de SIC
	Há apoio ativo à Segurança da Informação por parte da alta administração?	X		
	As atividades de Segurança da Informação são coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes?	X		
	Há uma definição clara das atribuições de responsabilidade associadas à Segurança da Informação?	X		
	Os requisitos para confidencialidade ou acordos de não divulgação que refletem as necessidades da organização para a proteção da informação são identificados e analisados criticamente?		X	
	Há um contato com autoridades e grupos de interesses especiais?	X		SISP/MPOG GSIC/PR
	São realizadas análises críticas/revisões dos objetivos de controle, controles, processos e procedimentos de segurança da informação a intervalos planejados e quando ocorrem mudanças significativas?		X	

	Há identificação dos riscos no acesso de prestadores de serviço?		X	
	Há controle de acesso específico para os prestadores de serviço?	X		IN04/MTUR POSIC/MTUR
	Há requisitos de segurança dos contratos de terceirização?	X		Verificar grau de exigência
GESTÃO DE ATIVOS	Há um inventário dos ativos físicos, tecnológicos e humanos?	X		
	Os ativos estão associados a proprietários?	X		PDSIC
	Há regras que delimitam o uso aceitável dos ativos?	X		IN4/MTUR POSIC/MTUR
	Há critérios de Classificação da Informação?		X	Planejamento Estratégico - Criação da Política de Classificação da Informação
SEGURANÇA EM RECURSOS HUMANOS	Há papéis e responsabilidades de Segurança da Informação definidos e documentados que devem ser cumpridos por funcionários, fornecedores e terceiros?		X	
	Há critérios de seleção e política de pessoal?	X		
	Há um acordo de confidencialidade, termos e condições de trabalho?	X		
	Há treinamento apropriado em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais para os usuários?		X	Condução de programa para Gestão de Segurança da Informação e Comunicações
	Há estrutura para notificar e responder aos incidentes e falhas de segurança?		X	Planejamento Estratégico - Criação da ETIR
	Há processos de encerramento de atividades, devolução de ativos e retirada de direitos de acesso?	X		Processo ineficaz
SEGURANÇA FÍSICA E DO AMBIENTE	Há uma definição de perímetros e controles de acesso físico aos ambientes?	X		Definição pode ser melhorada
	Há proteção contra ameaças externas e do meio ambiente?	X		
	Há recursos para segurança e manutenção dos equipamentos?	X		
	Há estrutura para fornecimento adequado de energia?	X		
	Há segurança no cabeamento?	X		
	Há um processo para retirada de equipamentos, informações ou software do local?	X		
GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES	Há procedimentos e responsabilidades operacionais?	X		
	Há controle de mudanças operacionais?		X	Falta de documentação e padronização

	Há segregação de funções e ambientes?	X		
	Há separação dos recursos de desenvolvimento, de teste e de produção?	X		
	Há um processo de controle da entrega de serviços terceirizados?	X		
	Há um processo de monitoramento, análise crítica e auditoria dos serviços terceirizados?		X	
	Há um processo de gerenciamento de mudanças para serviços terceirizados?		X	Falta de documentação e padronização
	Há planejamento e aceitação de sistemas?	X		
	Há controles contra códigos maliciosos e contra códigos móveis não autorizados?	X		Falta de documentação e padronização
	Há procedimentos para cópias de segurança?	X		Falta de documentação
	Há controles e gerenciamento de rede?	X		Falta de documentação
	Há mecanismos de segurança e tratamento de mídias?		X	Falta de documentação e padronização
	Há procedimentos para documentação de sistemas e segurança desta documentação?		X	Falta de documentação e padronização
	Há políticas, procedimentos e controles para proteger a troca de informações em todos os tipos de recursos de comunicação (inclusive correio eletrônico e sistemas de informações do negócio)?		X	
	Há controles para proteger as transações on-line de transmissões incompletas, erros de roteamento, duplicação ou reapresentação de mensagem não autorizada etc?	X		Falta de documentação e padronização
	Há controles para proteger a integridade das informações disponibilizada em sistemas publicamente acessíveis?	X		
	Os registros (log) para auditoria que contém atividades de usuários, exceções e outros eventos de segurança da informação são produzidos e mantidos em segurança por um determinado período de tempo acordado?	X		Falta de documentação e padronização
	Há processos de monitoramento e análise crítica da utilização dos recursos de processamento da informação?	X		Falta de documentação e padronização
	Os relógios dos sistemas de processamento de informações	X		Falta de documentação e padronização

	relevantes, dentro da organização ou do domínio de segurança, estão sincronizados de acordo com a hora oficial?			
CONTROLE DE ACESSO	A política de controle de acesso é baseada em requisitos do negócio?	X		Definição pode ser melhorada
	Há gerenciamento de acessos dos usuários?	X		Falta de documentação apropriada, padronização e processo de inclusão, remoção e atualização de permissões
	Os usuários são orientados a seguir boas práticas de segurança da informação na seleção e uso de senhas?		X	
	Há políticas de mesa limpa e tela limpa?		X	
	Há controle de acesso à rede?	X		
	Há controle de acesso ao sistema operacional?	X		
	Há controle de acesso às aplicações?	X		
	Há ambientes computacionais dedicados para sistemas sensíveis?		X	
	Há critérios para computação móvel e trabalho remoto?		X	
AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO	Há requisitos de segurança de sistemas?	X		Falta de documentação e padronização
	Há controles que previnam a ocorrência de erros, perdas, modificação não autorizada ou mal uso de informações em aplicações?		X	
	Há controles de criptografia?		X	
	Há controles de proteção que garantam a segurança dos arquivos de sistemas operacionais, de dados de teste e código-fonte?	X		Falta de documentação e padronização
	Há mecanismos de segurança nos processos de desenvolvimento e suporte?	X		Falta de documentação e padronização
	Há gerenciamento de vulnerabilidades técnicas?	X		Falta de documentação e padronização
GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	Há um processo de comunicação que notifica sobre fragilidades e eventos de segurança da informação associados aos sistemas de informação?	X		Falta de documentação e padronização
	Há um processo de gestão de incidentes de segurança da informação e melhorias?		X	Planejamento Estratégico - Criação da ETIR

GESTÃO DA CONTINUIDADE DO NEGÓCIO	Há um processo de gestão da continuidade do negócio que considera à segurança da informação?		X	
CONFORMIDADE	Há uma gestão de conformidades técnicas e legais?	X		Falta de documentação e padronização
	Há recursos e critérios para auditoria de sistemas?		X	

Tabela 14 – Checklist para verificação de Conformidade com a Norma ABNT NBR ISO/IEC 27002

Garantir que todo o ambiente tecnológico esteja completamente operacional é uma das principais missões de toda área de Tecnologia e Segurança da Informação. Atuar de forma proativa e em total sintonia com as necessidades do negócio é o que diferencia as empresas que obtêm sucesso em sua estratégia de continuidade de negócios.

4.2 Plano de Metas e Ações

A partir do "*Checklist* para verificação de Conformidade com a Norma ABNT NBR ISO/IEC 27002", das recomendações do Gabinete de Segurança Institucional da Presidência da República e demais órgãos de controle, foram definidas metas e ações prioritárias relacionadas à Segurança da Informação e Comunicações, imprescindíveis para implementar processos recorrentes da Gestão de Segurança da Informação e Comunicações – GSIC. O resultado está compilado na Tabela 15:

META	AÇÃO
Estabelecer a política de Classificação da Informação de forma a proteger adequadamente as informações no MTur, de sua propriedade ou sob sua custódia, contra revelação, adulteração e destruição.	Elaboração da Política de Classificação da Informação.
Definir e formalizar os procedimentos de resposta a incidentes de segurança de forma a orientar a ETIR do MTur frente a eventuais ações adversas, quanto ao procedimento de alerta, reação, contenção e tratamento.	Criação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais; Elaboração do Plano de Gestão para Tratamento e Resposta a Incidentes em Redes Computacionais.
Proceder à elaboração das Normas e Procedimentos complementares à Política de Segurança da Informação e Comunicações do MTur.	Deverão ser desenvolvidas as seguintes normas: • Dicionário de Termos Técnicos. • Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas; • Norma de Áreas Seguras; • Norma de Criação e Manutenção de Contas e Senhas;

META	AÇÃO
	• Norma de Gestão de Incidentes de Segurança da Informação e Comunicações; • Norma de Monitoramento; • Norma de Segurança Física de Instalações; • Norma de Segurança para Acordo de Nível de Serviço; • Norma de Segurança para Conformidade Legal; • Norma de Segurança para Equipamentos, Servidores e de Conectividade; • Norma de Segurança para Recursos Humanos e Partes Externas; • Norma de Segurança para Tratamento de Mídias e Backup; • Norma de Segurança para Uso de Correio Eletrônico; • Norma de Segurança para Uso de Internet; • Norma de Troca de Informação; • Norma Geral de Segurança da Informação para Técnicos; • Norma Geral de Segurança da Informação para Usuários; • Termo de Confidencialidade e Sigilo; • Termo de Custódia de Equipamento.
Realizar treinamentos que visem capacitar o Núcleo de SIC, o Grupo de Trabalho de SIC e demais pessoas envolvidas no processo de Gestão da Segurança da Informação e Comunicações do MTur.	Cursos a serem disponibilizados: • Formação em Security Officer: Módulo 1 • Auditor Líder em Segurança da Informação ISO 27001 • Gestão de Riscos • Tratamento e Resposta a Incidentes • Gestão da Continuidade de Negócios Elaboração do Plano de Capacitação em SIC.
Identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibra-los com os custos operacionais e financeiros envolvidos do Órgão	Definição do processo de Gestão de Risco de SIC; Elaboração do Plano de Gestão de Riscos.

Tabela 15 – Metas e Ações

4.3 Política de Classificação da Informação

De acordo com a Norma Complementar nº 07/IN01/DSIC/GSIPR, de 06 de maio de 2010, "*a identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso nos órgãos ou entidades da APF*". E que, *"para implementar os controles de acesso aprovados é fundamental a elaboração e divulgação de normas, bem como programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e Comunicações dos órgãos ou entidades da APF".*

A Classificação da Informação deverá ser implantada no MTur, em conformidade às legislações vigentes no País. Para tanto, adequações deverão ser previstas em uma Política de Classificação da Informação a ser elaborada pelo Ministério.

Esta Política será composta por regras que orientam o tratamento a ser dado às informações em todo seu ciclo de vida: criação, manipulação, transporte, armazenamento e descarte, categorizando-as de acordo com a sua relevância, e deverá ser baseado no Decreto nº 7.845, de 14 de novembro de 2012, na qual regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

4.4 Normas e Procedimentos de SIC

A Norma Complementar Nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, atribui ao Gestor de Segurança da Informação e Comunicações do órgão a responsabilidade de *"propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF".* E também, ao Comitê de SIC, *"propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema".* Cita ainda que "*a POSIC poderá ser complementada por Normas e Procedimentos que a referenciem*".

Em conformidade à POSIC do MTur e à legislação vigente referente ao tema, o Ministério do Turismo elaborará Normas e Procedimentos específicos em complemento a Política de Segurança da Informação e Comunicações cujo objetivo é o estabelecimento, o direcionamento e os princípios a serem adotados na Gestão de SIC do Ministério do Turismo, de forma a preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações do Órgão.

Deverão ser desenvolvidas as seguintes normas:

- Dicionário de Termos Técnicos.
- Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas;
- Norma de Áreas Seguras;
- Norma de Criação e Manutenção de Contas e Senhas;
- Norma de Gestão de Incidentes de Segurança da Informação e Comunicações;
- Norma de Monitoramento;
- Norma de Segurança Física de Instalações;
- Norma de Segurança para Acordo de Nível de Serviço;
- Norma de Segurança para Conformidade Legal;
- Norma de Segurança para Equipamentos, Servidores e de Conectividade;
- Norma de Segurança para Recursos Humanos e Partes Externas;
- Norma de Segurança para Tratamento de Mídias e Backup;

- Norma de Segurança para Uso de Correio Eletrônico;
- Norma de Segurança para Uso de Internet;
- Norma de Troca de Informação;
- Norma Geral de Segurança da Informação para Técnicos;
- Norma Geral de Segurança da Informação para Usuários;
- Política de Classificação da Informação;
- Termo de Confidencialidade e Sigilo;
- Termo de Custódia de Equipamento.

4.5 Plano de Capacitação – Núcleo de SIC e Grupo de Trabalho de SIC

Conforme Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, para a institucionalização da POSIC no órgão ou entidade da APF, deve-se promover a cultura de Segurança da Informação e Comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização.

Alinhado à Norma supracitada e a necessidade de capacitar o Núcleo de SIC, o Grupo de Trabalho de SIC e demais pessoas envolvidas, este projeto tem por objetivo sensibilizar, conscientizar, capacitar e treinar os colaboradores envolvidos no processo de Gestão da Segurança da Informação e Comunicações do MTur, de forma a reduzir os riscos voltados às pessoas.

Dentre os projetos previstos para atendimento deste objetivo inclui-se:

- Realizar treinamentos específicos aos membros do Núcleo de SIC, do Grupo de Trabalho de SIC e demais pessoas envolvidas;
- Elaborar cronograma anual de capacitação e treinamento para os usuários do MTur;
- Capacitar usuários em conceitos de Segurança da Informação e disseminar a cultura de SIC;
    - ✓ Palestras e congressos;
    - ✓ E-mail, Intranet e distribuição de panfletos de SIC.
- Elaborar Plano de Campanha de Sensibilização e Conscientização em SIC;
- Elaborar, aprovar e adquirir material para Marketing interno referente ao tema SIC.

Na área de Segurança da Informação, a capacitação é fundamental para a continuidade do suporte às ações do MTur. As necessidades de capacitação foram organizadas baseadas na prioridade de capacitação e pode ser ajustadas de acordo com as necessidades do órgão no momento de sua realização. Para cada capacitação necessária foi estimado um número, mínimo, de servidores que farão o curso, este número também foi baseado na prioridade de cada capacitação. A Tabela 16 relaciona as necessidades de capacitação do Ministério do Turismo para 2013/2015.

ÁREA DE CAPACITAÇÃO / CURSO	QUANTIDADE DE SERVIDORES	CARGA HORÁRIA	VALOR UNITÁRIO	VALOR TOTAL
Segurança – Gestão de Segurança da Informação e Comunicações	21	40h	2.750,00	57.750,00
Segurança – Auditor Líder em Segurança da Informação ISO 27001	21	40h	1.990,00	41.790,00
Segurança – Gestão de Riscos	21	16h	1.750,00	36.750,00
Segurança – Tratamento e Resposta a Incidentes	05	40h	2.300,00	11.500,00
Segurança – Gestão da Continuidade de Negócios	21	16h	790,00	16.590,00
TOTAL				164.380,00

Tabela 16 – Necessidades de Capacitação em SIC

4.6 Plano de Gestão de Riscos

A Norma Complementar nº 04/IN01/DSIC/GSIPR, de 15 de fevereiro de 2013, estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal - APF, direta e indireta.

De acordo com a NC04 "*as diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão ou entidade da APF, direta e indireta, além de estarem alinhadas à respectiva Política de Segurança da Informação e Comunicações do órgão ou entidade*". E que "*o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações*".

Alinhado ao modelo PDCA (*Plan-Do-Check-Act*), definido na Norma Complementar nº 02/DSIC/GSIPR de 14 de outubro de 2008, e com o objetivo de fomentar a melhoria contínua, o Ministério do Turismo elaborará um

Plano de Gestão de Riscos para identificar os principais riscos que podem afetar total ou parcialmente a execução das suas ações, impactando no alcance das metas e na realização das atividades do Órgão.

Para isso será mapeado o Processo de Gestão de Riscos de acordo com as recomendações da Norma Complementar nº 04/IN01/DSIC/GSIPR e no Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (Brasil/GSIPR, 2010). Também será aberto um Projeto, seguindo a metodologia do Escritório de Projetos do MTur, para elaborar o Plano de Gestão de Riscos de acordo com o Processo de Gestão de Riscos mapeado.

A sistematização do processo de avaliação de riscos permitirá a priorização dos riscos e ações, maior conhecimento sobre os riscos, mecanismos para obtenção de consenso, embasamento para as proteções atuais, entre outros benefícios. Com isso será possível identificar preliminarmente os riscos de maior criticidade, mensurar o potencial de impacto e a probabilidade de ocorrência, determinar as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir ou reter o risco. Alcançando, com isso, o objetivo que é manter os riscos em níveis aceitáveis no Órgão.

Para a elaboração desse Plano de Gestão de Riscos é recomendada a realização de análise da viabilidade de contratação de consultoria e de aquisição de ferramenta para gerenciamento de riscos.

4.7 Fatores Críticos de Sucesso

Os Fatores Críticos de Sucesso são as condições que precisam, necessariamente, serem satisfeitas para que o PDSIC tenha sucesso, tais como: credibilidade, compromisso e aceitação. Esses fatores precisam ser observados, tornando-se condições fundamentais a serem cumpridas para que este Plano Diretor alcance seus objetivos.

No que tange o Ministério do Turismo, foram elencados os seguintes pontos:

- Patrocínio da alta direção;
- Participação ativa do Comitê de Segurança da Informação e Comunicações;
- Política de Segurança da Informação e Comunicação do MTur implantada;
- Controle e acompanhamento dos Projetos e Ações derivados do PDSIC;
- Processo de Gestão de Riscos mapeado;

- Disponibilidade orçamentária e de recursos humanos;
- Conhecimento e alinhamento à IN01, IN02, IN03 e Normas Complementares – GSI/PR por parte de todo o Ministério;
- Continuidade de gestão de SIC;
- Capacitação dos servidores em Segurança da Informação;
- Conformidade às diretrizes dos Escritórios de Projetos e de Processos do MTur;
- Criação de uma estrutura organizacional dedicada aos processos de SIC;
- Responsabilidades bem definidas.

5 Conclusão

Para efetivação de uma Gestão de Segurança da Informação e Comunicações com seus respectivos requisitos e controles é necessário um trabalho conjunto. BASTOS e CAUBIT (2009, p. 31) citam que:

> *"De acordo com a norma ISO 27001, a organização deve estabelecer, documentar, implementar e manter um Sistema de Gestão de Segurança da Informação – SGSI (ou ISMS em inglês), sendo que este deve identificar os ativos a serem protegidos, a abordagem para gerenciamento dos riscos, os objetivos e controles necessários para proteger as informações da organização e garantir a continuidade do negócio no grau de qualidade requerido pela organização".*

Visto que o tema Segurança da Informação é amplo e que as leis, normas, políticas e melhores práticas fornecem orientação sobre Gestão de Segurança da Informação e Comunicações, o PDSIC foi desenvolvido com foco nas Normas Complementares publicadas pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR.

Apesar de o MTur possuir seus dispositivos de Segurança da Informação, o Órgão não possui uma estrutura adequada que garanta a permanente atualização, adequação e avaliação de efetividade de seus ativos, o Plano Diretor auxiliará na adequação entre a estrutura atual da instituição e as normativas publicadas pelo Gabinete de Segurança Institucional da Presidência da República. Utilizando-se os conceitos existentes sobre

o tema, as leis e as melhores práticas de Segurança da Informação o PDSIC será um referencial para a adequada implantação de uma Gestão de Segurança da Informação e Comunicações seguindo as recomendações existentes dentro de uma visão sistêmica. Essa sistematização será imprescindível para o sucesso de uma implementação de Segurança da Informação no Ministério do Turismo, pois trará muitos benefícios para o Órgão.

6 Referências

- ABNT NBR ISO/IEC 17799:2005 (27002). Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
- ABNT NBR ISO/IEC 27001:2006– Tecnologia da informação – Técnicas de segurança – Sistemas de Gestão da Segurança da Informação - Requisitos.
- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
- ABNT NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
- ABNT NBR ISO/IEC 27005:2011 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
- BASTOS, Alberto. ISO 27001 e 27002: gestão de segurança da informação - uma visão prática / Alberto Bastos; Rosângela Caubit; Porto Alegre, RS: Zouk, 2009.
- Constituição da República Federativa do Brasil de 1988.
- Decreto nº 1.171, de 22 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.
- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Decreto nº 7.845, de 14 de novembro de 2012, regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
- Guia de referência para a segurança das infraestruturas críticas da informação versão 01 – nov./2010
- Instrução Normativa GSI nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta e demais normas complementares.

- Instrução Normativa GSI nº 02, de 05 de fevereiro de 2013, que dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.
- Instrução Normativa GSI nº 03, de 06 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.
- Lei 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civil da União, das autarquias e das fundações públicas federais.
- Norma Complementar 01/IN02/NSC/GSIPR, de 28 de junho de 2013, que disciplina o Credenciamento de Segurança de Pessoas Naturais, Órgãos e Entidades Públicas e Privadas para o Tratamento de Informações Classificadas.
- Normas Complementares a Instrução Normativa Nº 01 - GSI/PR.
- Portaria n° 344, de 26 de outubro 2012, que institui Comitê de Segurança da Informação e Comunicações - CSIC e dispõe sobre suas competências, no âmbito do Ministério do Turismo.
- Portaria n° 108, de 22 de maio 2013, que institui a Política de Segurança da Informação e Comunicação - POSIC, no âmbito do Ministério do Turismo.
- Resolução nº 02, de 13 de novembro de 2012, que aprova o Regimento Interno do Comitê de Segurança da Informação e Comunicações do Ministério do Turismo.
- Resolução nº 03, de 29 de maio de 2013, que institui o Grupo de Trabalho de Segurança da Informação e Comunicações, no âmbito do Ministério do Turismo.
- Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário: Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal: Sumários Executivos. Brasília, 2008. Disponível em: <http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/tecnologia_informacao/sumarios/Sumario_Governan%C3%A7a%20em%20TI_miolo.pdf>.
- Tribunal de Contas da União. Acórdão 461/2004-TCU-Plenário: Identificação do Lote/Processo 014.147/2002-0/Código 37449551, disponível no site http://www.tcu.gov.br/

COGEP

BOLETIM

DE PESSOAL E SERVIÇO

Ministério do Turismo

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Edição Especial de Dezembro– Ano XI
Brasília-DF, 20 de dezembro de 2013

INFORMATIVO DE CIRCULAÇÃO INTERNA DO MINISTÉRIO DO TURISMO
PRODUZIDO PELA COORDENAÇÃO-GERAL DE GESTÃO DE PESSOAS - COGEP

Gastão Dias Vieira
Ministro de Estado do Turismo

Sergio Braune Solon de Pontes
Secretário-Executivo

Rubens Portugal Bacellar
Subsecretário

Célia Alves de Melo
Coordenadora-Geral de Gestão de Pessoas