GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

ARTEFATO POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

SECRETARIA DE COORDENAÇÃO E GOVERNANÇA DAS EMPRESAS ESTATAIS

DIRETORIA DE ORÇAMENTO DE ESTATAIS

COORDENAÇÃO-GERAL DE GESTÃO DA INFORMAÇÃO DE ESTATAIS

BRASÍLIA - 2018

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
SECRETARIA DE COORDENAÇÃO E GOVERNANÇA DAS EMPRESAS ESTATAIS

Fernando Antonio Ribeiro Soares
Secretário

André Nunes
Diretor do Departamento de Orçamento de Estatais

Gerson Batista Pereira
Coordenador-Geral de Gestão da Informação de Estatais

EQUIPE TÉCNICA
Natal Henrique Troz Guglilhermi – SEST
Otávio Porto Barbosa – SEST

UNIVERSIDADE DE BRASÍLIA

Márcia Abrahão Moura
Reitora

Sanderson Cesar Macedo Barbalho
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Georges Daniel Amvame Nze (Pesquisador Sênior)
Claudia Jacy Barrenco Abbas (Pesquisador Sênior)
Edna Dias Canedo (Pesquisador Sênior)
Rodrigo de Souza Goncalves (Pesquisador Sênior)
Adyr Andrade de Menezes
Amanda Aline Figueiredo Carvalho
Bruno Justino Garcia Praciano
Demétrio Antônio da Silva Filho
Fabricio de Oliveira Taguatinga
Glauber Luiz Lopes da Silva
Jean Victor Ribeiro Vieira
João Batista Alves Diniz
Jorge Guilherme Silva dos Santos
José Maria dos Reis Lisboa
Leomar Camargo de Souza
Marcus Vinicius Bomfim Guimaraes Barbalho
Moramay Coutinho Guimarães Coelho
Pedro Thiago Rocha de Alcântara
Priscilla Gonçalves da Silva e Souza
Rafaella Aparecida Rosa Lima
Rosa Cristina Portela Dias Jácome
Ruyther Parente da Costa
Victor Matheus da Silva

B823g
Brasil. Ministério do Planejamento, Desenvolvimento e Gestão.

Governança de tecnologia da informação : artefato política de segurança da informação e comunicação / Ministério do Planejamento, Desenvolvimento e Gestão, Secretaria de Coordenação e Governança das Empresas Estatais, Coordenação-Geral de Gestão da Informação de Estatais; Universidade de Brasília. -- Brasília : MP, 2018.
14 p.

1. Governança Digital 2. Tecnologia da Informação 3. Empresa Estatal 4. Administração Pública I. Título II. Universidade de Brasília.

CDU 658.115:004

HISTÓRICO DE VERSÕES

26/03/2018 | Versão 1.0

Descrição: Inclusão dos artefatos, definição do processo, adequação do passo-a-passo, objetivos e capa ao processo.

Autor: Edna Dias Canedo e Pedro Thiago Rocha de Alcântara.

Revisor: Natal Henrique Troz Guglilhermi e Otávio Porto Barbosa.

SUMÁRIO

INTRODUÇÃO

Em observância às normas e diretrizes de Tecnologia da Informação (TIC) do Poder Executivo Federal, disseminadas pela Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão (SETIC/MP), na condição de Órgão Central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e, conforme preconiza o Decreto Presidencial nº 7.579, de 11 de outubro de 2011, o Ministério do Planejamento, Desenvolvimento e Gestão (MP), como Órgão Setorial integrante do SISP, vincula-se aos preceitos definidos pelo Sistema relativamente à governança e gestão de tecnologia da informação.

Diante do tema e também em decorrência de orientação do TCU, conforme Acórdão 3051/2014 a SEST deve atuar no desenvolvimento de ações que promovam a disseminação da cultura de Governança de TIC nas Empresas Estatais, para facilitar o cumprimento dos objetivos definidos e exigidos no planejamento estratégico, como também na racionalização de recursos e retorno financeiro/operacional.

VISÃO GERAL

2.1. Objetivo

Identificar e apontar os passos necessários, de acordo com práticas listadas em literatura e conhecimento prático, para a Política de Segurança da Informação e Comunicação nas diferentes Empresas Estatais.

2.2. Justificativa

A SEST, institucionalmente, como órgão de Coordenação e Governança das Empresas Estatais, deve promover e orientar a Governança de TIC dessas entidades. As iniciativas nesse sentido devem ser planejadas e priorizadas a partir do alinhamento dos investimentos de TIC aos objetivos estratégicos das organizações.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

3.1. Definição

A Política de Segurança da Informação e Comunicação visa proteger a informação da estatal para manter um nível aceitável de risco de segurança da informação, em linha com a política de segurança.

Para isso, faz-se necessários estabelecer e manter papéis e privilégios de acesso a informação.

3.2. Passo a passo

Para implantação da Política de Segurança da Informação e Comunicação, é preciso executar as seguintes atividades:

1 - Proteger as informações de propriedade e/ou sob a guarda da Estatal, seja a informação física ou lógica.

2 - Proteger a Estatal contra software malicioso.

3 - Gerenciar a segurança das conexões de rede e conectividade da Estatal.

4 - Gerenciar a segurança dos endpoints (pontos de acesso) da Estatal.

5 - Gerenciar identidade de usuários e acessos lógicos da Estatal.

6 - Gerenciar acesso físicos e lógicos aos ativos de TIC da Estatal.

7 - Gerenciar o manuseio dos documentos sensíveis e dispositivos de saída da Estatal.

8 - Monitorar a infraestrutura da Estatal por eventos de segurança.

9 -Classificar o nível da sensibilidade da informação da Estatal.

ARTEFATOS

4.1. Documentos

Os modelos dos documentos para Política de Segurança da Informação e Comunicação, estão disponíveis para download no endereço eletrônico http://www.planejamento.gov.br/acesso-a-informacao/institucional/unidades/sest, conforme lista a seguir:

Definir Política de Segurança	
 Política de Segurança da Informação e Comunicação	Nome: Política de Segurança da Informação e Comunicação
	Objetivo: Documentar Política de Segurança da Informação e Comunicação definida.
Definir Papéis e Privilégios de Acesso	
 Formulário de Definição dos Papéis e Privilégios de Acesso	Nome: Formulário de Definição dos Papéis e Privilégios de Acesso
	Objetivo: Documentar os Papéis e Privilégios de Acesso definidos.
Classificar a Informação	
 Formulário de Classificação da Informação	Nome: Formulário de Classificação da Informação
	Objetivo: Documentar as Classificação da Informação definidas.

4.1.1 Política de Segurança da Informação e Comunicação

Política de Segurança da Informação e Comunicação da <Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Introdução

<Introduzir a política de segurança, ressaltando seu papel na organização.>

2. Autenticação

<Apresentar política de autenticação>

2.1. Política de Senha
<Detalhar política de senha>

2.2. Política de E-mail
<Detalhar política de uso de e-mail.>

2.3. Política de Acesso a Internet
<Descrever a política de acesso a internet.>

3. Política de uso de Estação de Trabalho
<Descrever a política de segurança em relação a uso de estações de trabalho. >

4. Política Social
<Descrever fatores sociais da política de segurança.>

5. Vírus e Códigos Maliciosos
<Descrever a política de segurança em relação a vírus e códigos maliciosos>

6. Equipe de Segurança
<Descrever a equipe de segurança>

6.1. Membros da Equipe Técnica
<Listar Membros da Equipe Técnica.>

Nome	E-mail	Ramal	Celular

6.2. Membros da Equipe de Segurança
<Listar Membros da Equipe de Segurança.>

Versão	E-mail	Ramal	Celular

Aprovado em ___ de _____ de _____.

<Nome completo do responsável>
<Cargo >

4.1.2 Formulário de Definição dos Papéis e Privilégios de Acesso

Formulário de Definição dos Papéis e Privilégios de Acesso
<Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Objetivo
<Descrever o objetivo do Formulário de Definição dos Papéis, Responsabilidades, Competências e Privilégios de Acesso e Níveis de Autoridade>

2. Conceitos e Definições
<Listar e definir os conceitos importantes para o entendimento do Formulário>

3. Definição dos Papeis, Responsabilidades e Competências
<Listar os papeis e atribuir responsabilidades e caracteriza-los.>

4. Privilégios de Acesso
<Descrever os privilégios de acesso de cada papel definido>

Aprovado em ___ de _____ de _____.

<Nome completo do responsável>
<Cargo>

Observações: Em segurança, especialmente segurança física, o termo controle / privilégio de acesso é uma referência à prática de permitir o acesso a uma propriedade, prédio, ou sala, apenas para pessoas autorizadas. O controle físico de acesso pode ser obtido através de pessoas (um guarda, segurança ou recepcionista); através de meios mecânicos como fechaduras e chaves; ou através de outros meios tecnológicos, como sistemas baseados em cartões de acesso.

O controle/privilégio de acesso, na segurança da informação, é composto dos processos de autenticação, autorização e auditoria (Accounting). Neste contexto o controle de acesso pode ser como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo). A autenticação identifica quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer, e a auditoria diz o que o usuário fez.

O controle de acesso discricionário são uma política de controle de acesso determinada pelo proprietário do recurso (um arquivo, por exemplo). O proprietário do recurso decide quem tem permissão de acesso em determinado recurso e qual privilégio ele tem.

Existem dois conceitos importantes:

- Todo objeto em um sistema deve ter um proprietário. A política de acesso é

determinada pelo proprietário do recurso. Teoricamente um objeto sem um proprietário é considerado não protegido.

- Direitos de acesso são estabelecidos pelo proprietário do recurso, que pode inclusive transferir essa propriedade.

No controle de acesso obrigatório a política de acesso é determinada pelo sistema e não pelo proprietário do recurso. Este controle é utilizado em sistemas cujos dados são altamente sensíveis, como governamentais e militares.

Em sistemas de controle de acesso obrigatório, todos os envolvidos e objetos devem ter rótulos associados. Um rótulo de sensibilidade de um envolvido define o seu nível de confiança. Um rótulo de sensibilidade de um objeto define o nível de confiança necessário para acessá-lo. Para acessar um determinado objeto, o envolvido deve ter um rótulo de sensibilidade igual ou superior ao requisitado pelo objeto.

Dois métodos são comumente utilizados na aplicação de controle de acesso obrigatório:

Controles baseados em regras. Todos os sistemas implementam uma forma simples de controle de acesso baseado em regras que define que o acesso deve ser dado ou negado com base no:

- Rótulo de sensibilidade do objeto

- Rótulo de sensibilidade do envolvido.

Um controle baseado em papéis é uma abordagem para restringir o acesso a usuários autorizados. Controles de acesso baseados em papéis (roles) definem os direitos e permissões baseados no papel que determinado usuário desempenha na organização. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários.

Permissões de acesso e direitos sobre objetos são dados para qualquer grupo ou, em adição, indivíduos. Os indivíduos podem pertencer a um ou mais grupos. Os indivíduos podem adquirir permissões cumulativas ou desqualificado para qualquer permissão que não faz parte de todo grupo à qual ele pertence.

Exemplos:

O Gestor da Política de Segurança da Informação e Comunicações deverá:

a) promover cultura de SIC na estatal;

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor recursos necessários às ações de SIC;

d) coordenar o Comitê de SIC;

e) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

f) manter contato direto com o departamento de SIC para o trato de assuntos relativos à SIC;

g) propor Normas Internas;

h) fornecer o suporte administrativo necessário à gestão da Posic.

O usuário é responsável pela segurança dos ativos e processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, tais como: crachá, token, login, senha eletrônica, certificado digital e endereço de correio eletrônico. Independentemente da adoção de outras medidas, o titular da estatal deverá, de imediato, comunicar todo incidente de SIC que ocorra no âmbito de suas atividades, mediante o envio de relatório circunstanciado.

4.1.3 Formulário de Classificação da Informação

Formulário de Classificação da Informação
<Sigla da estatal>

1. Identificação da Informação
<Identificar a informação a ser classificada no presente formulário>

2. Grau de Sigilo da Informação
<Classificar o grau de sigilo>

3. Justificativa da Classificação
<Justificar o grau de sigilo, colocar fundamentação legal se for o caso.>

4. Prazo para restrição de acesso
<Definir prazo para retirar restrição de acesso.>

Aprovado em ___ de _____ de _____.

<Nome completo do responsável>
<Cargo>

Observações:

A classificação da informação é certamente uma das partes mais atrativas da gestão da segurança da informação, mas ao mesmo tempo, uma das mais mal-entendidas. Isto provavelmente se deve ao fato de que historicamente, a classificação da informação foi o primeiro elemento da segurança da informação a ser gerenciado.

A principal norma de segurança da informação ISSO 27001 é a mais usada, embora a classificação possa ser feita de acordo com outro critério. Em termos de confidencialidade, a norma é o tipo mais comum de classificação da informação.

A boa prática diz que a classificação deve ser feita de acordo com o seguinte processo:

Inventário de ativos (Registro de ativo)

O propósito em se desenvolver um inventário de ativos é para a estatal saber quais informações classificadas ela tem em sua posse, e quem é responsável por elas (ou sejam seu proprietário).

Informação classificada pode estar em diferentes formatos e tipos de mídia, como por exemplo:

- Documentos eletrônicos
- Sistemas de informação / bases de dados
- Documentos em papel
- Mídias de armazenamento (ex.: discos, cartões de memória, etc.)
- Informação transmitida verbalmente
- E-mail.

Classificação da informação

A ISO 27001 não prescreve os níveis de classificação – isto é algo que a estatal deve desenvolver por conta própria, baseado no que é mais comum. Quanto maior e mais complexa for a estatal, mais níveis de confidencialidade terá – por exemplo, para estatal de médio porte pode utilizar este tipo de níveis de classificação da informação, com três níveis de confidencialidade e um nível público:

- Confidencial (o mais alto nível de confidencialidade)
- Restrita (médio nível de confidencialidade)
- Uso interno (o mais baixo nível de confidencialidade)
- Pública (todos podem ver a informação).

Em muitos casos, o proprietário do ativo é o responsável por classificar a informação – e isto é usualmente feito com base nos resultados da análise/avaliação de riscos: quanto maior o valor da informação (quanto maiores as consequências de uma quebra da confidencialidade), maior deve ser o nível de classificação.

Rotulagem da informação

Uma vez que tenha classificado a informação, é preciso rotulá-la apropriadamente – deve – se desenvolver orientações para cada tipo de ativo de informação sobre como ele

precisa ser rotulado – novamente, a ISO 27001 não é prescritiva, então deve-se desenvolver suas próprias regras.

Por exemplo, pode – se definir as regras para documentos em papel de tal forma que o nível de confidencialidade seja indicado no canto superior direito de cada página do documento, e que a classificação também seja indicada na capa ou no envelope que transporta tal documento, assim como na pasta onde o documento é armazenado. A rotulagem da informação geralmente é responsabilidade do proprietário da informação.

Manuseio de ativos

Esta é usualmente a parte mais complexa do processo de classificação – você deveria desenvolver regras sobre como proteger cada tipo de ativo dependendo do nível de confidencialidade. Por exemplo, você poderia usar uma tabela na qual você deve definir as regras para cada nível de confidencialidade para cada tipo de mídia, por exemplo:

Tipo	Uso Interno	Restrito	Confidencial	
Documentos Eletrônicos				
Documentos em Papel				
Mídia de Armazenamento				
Sistemas de Informação				
E-mail				

REFERÊNCIAS BIBLIOGRÁFICAS

5.1. Documentos

- Planejamento Estratégico da Secretaria 2015-2018.
- Guia de Comitê de TIC do SISP (versão 2.0 – 2016).
- Guia do PDTIC do SISP (Versão 2.0 Beta – 2015).
- Guia de Gerenciamento de Projetos do SISP (Versão 1.0 MGP-SISP – 2011).

- Guia de Metodologia de Gerenciamento de Portfólio de Projetos do SISP (Versão 1.0 MGPP-SISP – 2013).
- Guia de Processo de Software do SISP (Versão 1.0 PSW-SISP 2012).
- Guia de Governança de Tecnologia da Informação e Comunicação (GovTIC) do SISP (Versão 2.0 - 2017).