NORMA TÉCNICA
ATI-SGR-PR/001:13

Política de Segurança da Informação – Diretrizes Gerais

Versão 3.0

Válida a partir da publicação da Resolução 001/2013

Palavras-chave: Segurança, Informação, Diretrizes, Regras, Normas, Risco, Continuidade, Vulnerabilidade, Incidente, Ativo, Confidencialidade, Disponibilidade, Integridade, ATI.

Esse Documento é classificado como público

Agência Estadual de Tecnologia da Informação

23 páginas

Sumário

Prefácio

A Segurança da Informação é elemento fundamental para preservar a qualidade dos serviços prestados pela ATI, através da garantia da confidencialidade, disponibilidade e integridade das informações sob sua custódia.

A Política de Segurança da Informação é um instrumento base para todas as ações inerentes à Segurança da Informação e necessita de constante atualização. Essa versão 3.0 foi elaborada pela Unidade de Segurança da Informação – USI – da ATI, em conjunto com especialistas, redigida em conformidade com as convenções redacionais estabelecidas pela ATI [6] [7] e segundo os padrões nacionais e internacionais atualmente utilizados [1] [2] [3] [4] [5].

Esta Norma foi aprovada pelo Comitê Gestor de Segurança da Informação – CGSI [8] e substitui o documento intitulado Política de Segurança da Informação da ATI – PSI/ATI – Versão 2, de 2010.

1 Introdução

O uso da Tecnologia da Informação na Administração Pública envolve grande acervo de recursos computacionais e informações que necessitam estar permanentemente protegidos contra perda da confidencialidade, integridade e disponibilidade.

Como parte de um conjunto de medidas de segurança, torna-se necessária a definição e implantação pela ATI de um arcabouço normativo formado por uma Política de Segurança da Informação que estabeleça diretrizes gerais para a implantação de normas, regras, padrões e requisitos mínimos, nos diversos aspectos que envolvem direta e indiretamente, a manipulação, o trânsito e a guarda do acervo de informações que se utilizam da sua infraestrutura de tecnologia.

Esta Política tem como objetivo expressar, pública e formalmente, as preocupações da ATI com a informação, norteando e proporcionando subsídios e condições que assegurem níveis mínimos adequados de integridade, confidencialidade e disponibilidade das mesmas.

2 Escopo

Essa Norma tem o objetivo de padronizar e estabelecer requisitos mínimos, a fim de proporcionar condições que assegurem a integridade, a confidencialidade, a disponibilidade, bem como a legalidade da informação no âmbito do ambiente computacional da ATI.

As regras estabelecidas neste documento estendem-se a todos os que fazem parte da instituição, tais como empregados, servidores, cargos em comissão, terceirizados, estagiários, prestadores de serviços e os que, de alguma forma, fazem uso dos recursos computacionais da mesma.

Esta Política engloba não apenas os requisitos de segurança lógica, mas, também, os de segurança física e de pessoal nos ambientes computacionais.

3 Da Organização do Arcabouço Normativo

a) O arcabouço normativo no que concerne à segurança da informação é organizado e implementado minimamente como segue:

   1. Documento de Política de Segurança – PSI;
   2. Documentos normativos acessórios e outros documentos, conforme o caso e necessidade;

b) Deve-se manter permanente e forte aderência do conjunto normativo (PSI e seus documentos acessórios) tanto com as mudanças e necessidades de segurança dos ativos de informação, quanto da missão ou organização interna da ATI. Assim, tanto esta política quanto seus documentos acessórios devem ser periodicamente reavaliados e eventualmente

revistos sempre que ocorram eventos ou fatos relevantes que os demandem ou justifiquem;

c) A PSI e seus documentos acessórios aplicam-se, indistintamente, a todos os recursos humanos da instituição, próprios ou terceirizados, permanentes ou temporários, a qualquer título. Para tanto, o princípio da publicidade do conjunto normativo vigente deve ser aplicado, preferivelmente sob a forma de um programa continuado de divulgação e conscientização no elemento humano sobre a segurança da informação;

d) Os documentos normativos acessórios regulamentam a aplicação desta PSI no seio da instituição;

e) Os documentos normativos acessórios e suas decorrências deverão, como regra, recomendar ou implementar apenas normas técnicas, códigos de prática e outros procedimentos de segurança já normatizados por legislação vigente cabível hierarquicamente superior ou, caso inexistente, oriundas ou recomendadas por órgão ou entidade normativa técnica nacional ou internacional, de competência e aceitação amplamente reconhecidas;

f) Esta política (PSI) é pública, sem restrições quanto a confidencialidade. Seus documentos acessórios, por outro lado, tem como regra ser de uso restrito na instituição, caso a divulgação externa do seu teor represente, ou forneça subsídios para ameaças aos ativos de informação da ATI ou ao cumprimento de sua missão, respeitada a legislação em vigor;

   1. Eventuais exceções ou necessidades especiais que se apresentem requerem autorização prévia e expressa do gestor responsável,

observada a legislação pertinente;

2. Tanto a política quanto seus documentos acessórios devem ser amplamente divulgados ao público, através do recurso adequado, com controle discricionário de acesso em caso de informação de uso restrito, conforme o caso e necessidade, observadas as normas legais;

3. Campanhas de conscientização, treinamentos e outros recursos devem ser utilizados com frequência e conteúdo adequados à demanda de cada público.

4 Diretrizes Gerais

a) A aplicação desta Política de Segurança requer que seus efeitos sejam evidenciados, monitorados e controlados por um instrumento de gestão adequado.

   1. Um SGSI – Sistema de Gestão da Segurança da Informação – adequado com o disposto nesta PSI deverá ser mantido continuamente;

   2. O SGSI é o meio de controle que:

      i. Evidenciará que a PSI está sendo cumprida no nível tático operacional, pelo acompanhamento das ações e monitoramento de métricas, de forma fornecer subsídios para as ações de controle;

      ii. Fornecerá aos gestores as informações sobre a eficácia de suas ações, de forma manter os níveis de segurança dos ativos de informação dentro das expectativas da instituição, conforme o caso.

b) Os gestores da ATI, de qualquer nível da sua estrutura administrativa e

conforme o caso, são responsáveis por:

1. Fazer refletir de forma adequada e suficiente, em suas respectivas áreas de atuação e na forma da Lei, as diretrizes estabelecidas na PSI e seus documentos acessórios;
2. Usar os procedimentos técnico-administrativos adequados e cabíveis para propor e aperfeiçoar normas, procedimentos ou outros instrumentos afins, de forma a permitir o incremento da eficácia dos mesmos na aplicação da PSI e suas decorrências na sua área de atuação;
3. Por identificar na sua área de competência, promovendo as ações cabíveis e adequadas em cada caso:
    i. Riscos aos ativos de informação;
    ii. Oportunidades de disseminar o aculturamento do elemento humano na segurança dos ativos de informação;
    iii. Necessidades de implementação e oportunidades de uso adequado dos princípios doutrinários da segurança da informação na proteção dos ativos de informação;
4. Fornecer continuamente, no que lhe cabe, as informações necessárias e requeridas para alimentar o SGSI, bem como se utilizar destas para orientar suas ações futuras;
5. Usar dos meios administrativos cabíveis e adequados para reportar quaisquer informações, eventos ou situações que possam caracterizar não-conformidade com esta PSI e suas decorrências, ou que apontem redundar em riscos não controlados para os ativos de informação;

6. Cumprir e fazer cumprir a PSI e suas decorrências.

c) Não são permitidas quaisquer atividades envolvendo direta ou indiretamente ativos de informação que ponham em risco, sem controle adequado, a informação e outros ativos da instituição, salvo explicitamente permitidas por esta PSI, ou que tenha sido prévia e formalmente autorizada pelo setor ou gestor competente, conforme o caso;

d) É vedada a instalação e uso de quaisquer dispositivos, sistemas, informações ou outros recursos não autorizados, que violem propriedade intelectual ou comercial, alheios à missão da ATI ou que infrinjam norma legal.

5 Dos Requisitos de Segurança da Informação

a) Os ativos de informação:

1. São inventariados e permanentemente controlados para os seus diversos fins;

2. Possuem gestor responsável;

b) A informação da ATI é classificada de acordo com o seu grau de criticidade em relação aos pilares de confidencialidade, integridade e disponibilidade, observadas as necessidades do negócio e a legislação em vigor;

1. Quanto ao quesito confidencialidade recomenda-se minimamente o uso de três níveis:

i. Informação pública – Dados ou informações que devem ser divulgadas publicamente por força e na forma da Lei, ou que possa

ou precise ser divulgada, sem implicar em riscos, e por interesse ou necessidade da instituição no cumprimento de sua missão;

ii. Informação de uso interno – Dados ou informações que, por sua natureza, conteúdo ou exigência legal, caso divulgadas publicamente, possam representar risco ao cumprimento da sua missão;

iii. Informação restrita – Dados ou informações que, por exigência legal, sua própria natureza, conteúdo, exigência do ofício, praxe administrativa ou interesse da própria instituição para o cumprimento de sua missão, deve ser disponibilizada apenas internamente, com controle de acesso discricionário e apenas para parte do seu capital humano.

2. Informações sem classificação quanto à confidencialidade devem ser consideradas, como regra, de uso interno, até disposição administrativa ou legal em contrário;

3. Quanto aos requisitos de integridade e disponibilidade, recomenda-se minimamente os três níveis a saber:

   i. Baixa criticidade;

   ii. Média criticidade;

   iii. Alta criticidade;

c) Como regra, deve-se implementar mecanismos de proteção compatíveis com os níveis de criticidade requeridos por cada informação;

d) Os gestores da informação classificarão as informações e estabelecerão os

níveis de requisitos das mesmas;

e) Ativos de informação e quaisquer procedimentos que os envolvam herdam automaticamente o mesmo nível de criticidade da informação que contém, manipulam ou transportam.

6 Dos Princípios Doutrinários

a) São princípios doutrinários norteadores e que devem ser utilizados na implementação desta PSI, sempre que oportunidades se apresentarem, onde adequado e conforme o caso:

1. Tríade: Prevenção, Detecção e Resposta

   i. Prevenção – Procedimentos e outras medidas que implementem o princípio da pró-atividade na contenção das ameaças e na mitigação de vulnerabilidades, minimizando riscos;

   ii. Detecção – Procedimentos e outras medidas que, em face de eventual ineficácia ou complacência da abordagem preventiva, evidencie a ocorrência de incidente para o disparo de ações cabíveis, conforme o caso;

   iii. Resposta – Procedimentos, ações e outras medidas disparadas para a investigação de incidentes e determinação de suas causas, buscando fazer cessar ou mitigar seus efeitos e impactos, permitindo o levantamento de experiências e subsídios para o aprimoramento da prevenção e detecção, conforme o caso.

2. Compartimentalização e Segregação – Topologias, modelos de comunicação inter-dispositivos e funcionais, filtragens, políticas,

procedimentos, controle de acesso físico e discricionário ou ainda a implementação de recursos, funções administrativas ou outros meios que permitam confinar ameaças, vulnerabilidades e riscos, mitigando preventivamente que estes permeiem uniforme e indiscriminadamente o ambiente;

3. Auditabilidade e transparência – Geração contínua, adequada e suficiente de registros auditáveis, conforme o caso, de forma a permitir, a posteriori e por terceiros previamente autorizados, o monitoramento das operações bem como a consulta, investigação e eventual esclarecimento de eventos ou incidentes de qualquer natureza;
4. Simplicidade e Pragmatismo nas Ações – Preferência pela implementação de ações simples e eficazes em lugar de ações complexas ou apenas de eficácia nominal;
5. Defesa em Profundidade – Implementação de perímetros defensivos concêntricos ou sucessivos em um ativo de informação, de forma que a proteção ao ativo não seja única caso a ameaça venha a transpor a primeira linha defensiva. O princípio da defesa em profundidade, como regra, deve ser utilizado de forma conjugada com o princípio da diversidade de defesas;
6. Diversidade de Defesas – Política de impor desafios de naturezas distintas em esquemas defensivos sucessivos;
7. Proporcionalidade – Modulação que deve, como regra, nortear a natureza e intensidade das ações mitigadoras, de forma a manter uma proporção coerente entre os riscos e seus impactos, por um lado, e os

recursos efetivamente alocados para sua mitigação e seu controle, do outro;

8. Funcionalidade e privilégio mínimos – Política de somente permitir o acesso ou privilégios a funcionalidades e ativos de informação estritamente necessários e suficientes, tanto para os sistemas quanto para os usuários desempenhem suas funções;
9. Melhoria contínua – Princípio que busca o aperfeiçoamento contínuo de qualquer processo, sistema de processos ou procedimento, de forma a implementar um ciclo virtuoso de melhoria crescente;
10. Conformidade e Legalidade – Aderência a contratos, padrões normativos e legislação vigentes e cabíveis;

b) São cenários que devem ser evitados ou mitigados:

1. Ponto único de falha – Cenário que atenta usualmente contra a funcionalidade ou o desempenho, por não prever ou implementar níveis mínimos de resiliência ou redundância;
2. Segurança baseada em obscuridade como única defesa – Cenário que deve ser evitado, uma vez que além de não contemplar o princípio da defesa em profundidade, pressupõe a ineficácia da ameaça baseada apenas na sua eventual ignorância, além de usualmente gerar uma falsa sensação de segurança. A segurança por obscuridade pode e eventualmente deve ser utilizada, mas apenas como coadjuvante entre outros esquemas defensivos de eficácia menos controversa;
3. Responsabilidade indefinida ou coletiva – Cenário em que, ainda que apenas por hipótese, a falta de previsão adequada não permite

determinar inequivocamente a quem se atribuir uma ação ou omissão que deveria implicar em uma necessária e clara responsabilidade individual associada;

4. Ações apenas nominais – Ações caracteristicamente não pragmáticas e que aparentam eficácia apenas formal;
5. Conflitos de interesse – Situação em que um agente pode ser influenciado ou estimulado a agir de forma diversa da esperada por conta de outro interesse;

7 Dos Recursos e Meios para a Implementação das Abordagens Doutrinárias

a) Os recursos e meios a serem utilizados para a implementação das abordagens de prevenção, detecção e resposta são:

1. Tecnologia – Recurso formado por mecanismos, técnicas e dispositivos tecnológicos, adequados a cada caso, que permitam a eficácia e produtividade típicas destes para os fins desejados;
2. Pessoas – Recurso agregador da inteligência e experiência necessárias à qualidade do processo de implementação, de forma a se evitar as limitações inerentes aos recursos de tecnologia;
3. Processos – Recurso necessário para implementar a padronização das ações, com reflexos positivos na manutenção dos níveis de previsibilidade, coerência, aderência e nível de qualidade das mesmas.

b) Os recursos devem ser utilizados observando-se as necessidades específicas requeridas a cada caso.

8 Da Propriedade da Informação

a) Toda informação criada, manuseada, armazenada, processada, transportada, ou descartada pelo elemento humano direto ou indireto da ATI para o cumprimento de sua missão, seja na sua infraestrutura de TIC ou não, está sob custódia da mesma e deve ser protegida segundo as diretrizes aqui descritas e sem prejuízo da legislação vigente;

b) Quando da obtenção de informação de terceiros, o Gestor da Informação deve, como regra, providenciar junto ao concedente a documentação formal que implique em direito de acesso antes de seu uso efetivo;

c) Na hipótese de cessão de bases de dados de informação, custodiadas ou não, cabe ao gestor da informação emitir autorização expressa;

d) Não existirão ativos de informação sem gestor responsável.

9 Da Continuidade do Negócio

a) De forma a permitir o cumprimento de sua missão, deve-se monitorar e controlar o risco de interrupção de serviços causada por desastres ou falhas nos recursos de tecnologia da informação e comunicação que suportam as operações;

b) Os níveis de resiliência dos serviços que se utilizam de ativos de informação devem ser planejados e implementados por meio de um Plano de Continuidade do Negócio (PCN) levando-se em conta os danos potenciais ao negócio causados por indisponibilidade de qualquer natureza;

c) O Plano de Continuidade do Negócio deve ser testado periodicamente e aprimorado conforme a demanda;

10 Do Ambiente Físico

a) O ambiente físico da instituição é constituído pela totalidade do ativo permanente da instituição, quaisquer informações ou ativos de informação contornados pelos seus limites físicos, ou ainda delimitado por quaisquer ambientes em que residam suas informações ou ativos de informações, o que incluem os fornecedores de serviços, conforme o caso;

b) Os ativos de informação que sejam objeto de preocupação específica devem possuir dispositivos próprios para controle de acesso e auditoria;

c) Ativos de informação e outros recursos sensíveis são mantidos em áreas cuja proteção física é proporcional aos riscos aos quais estão submetidos, ao valor da informação a proteger, ou aos impactos previstos gerados na eventualidade de incidentes ou acidentes.

11 Penalidades

A não observância dos preceitos desta Política poderá implicar na aplicação de sanções administrativas, cíveis e penais previstas na legislação em vigor que regule ou venha regular a matéria.

12 Outras Disposições

a) Os processos que eventualmente envolvam certificação digital e certificados digitais de autoridades certificadoras e de registro (AC e AR)

deverão ser compatíveis com as políticas específicas vigentes das mesmas, conforme o caso e legislação em vigor;

b) O setor responsável deve ser acionado, pelas vias administrativas previstas, a qualquer tentativa (informada ou detectada) de violação do disposto na PSI e suas decorrências, que deve tomar as medidas previstas cabíveis e necessárias;

c) Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, a qualquer título, devem refletir esta PSI e seus documentos acessórios, sem prejuízo da observância da legislação em vigor;

d) Colaboradores indiretos e terceirizados desempenharão suas funções e executarão seus contratos sempre sob supervisão da área contratante, através de gestor definido, que zelará pela conformidade das atividades executadas com a PSI e seus documentos acessórios, conforme o caso;

e) Devem existir procedimentos para permitir que quando colaboradores, prestadores de serviços ou usuários em geral sejam transferidos, remanejados, estejam com contrato suspenso ou encerrado, afastados ou demitidos, tenham suas credenciais e privilégios de acesso revistos, suspensos ou revogados, conforme o caso e necessidade;

f) No descarte ou movimentação de informações ou ativos de informação devem ser observados as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação, conforme o caso;

13 Atribuições e Responsabilidades

Às estruturas de apoio, aos gestores, às chefias, aos analistas, aos técnicos e aos usuários dos ambientes, dos recursos, dos ativos de informação e dos ativos computacionais da ATI, cabem cumprir atribuições e assumir responsabilidades específicas, com relação à Segurança da Informação, segundo as suas competências.

14 Referências

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBRISO/IEC27001, Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos, mar. de 2006.

[2] ABNT. NBRISO/IEC27002, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação, ago. de 2005.

[3] ABNT. NBRISO/IEC27003, Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação, nov. de 2011.

[4] ABNT. NBRISO/IEC27004, Tecnologia da informação — Técnicas de segurança — Gestão da segurança da informação — Medição, mai. de 2010.

[5] ABNT. NBRISO/IEC27005, Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação, jul. de 2008.

[6] ATI. SEIG-GGT-PR/001-1:08. Versão 1.0 – Recife, 2009. Disponível em: <www.ati.pe.gov.br>. Acesso em: 02 de mai. de 2013.

[7] ATI. SEIG-GGT-PR/001-2:08. Versão 1.0 – Recife, 2009. Disponível em: <www.ati.pe.gov.br>. Acesso em: 02 de mai. de 2013.

[8] ATI. Portaria N° 033/2013 – Recife, 2008. Disponível em: <www.ati.pe.gov.br>. Acesso em: 14 de mai. de 2013.