NORMA TÉCNICA
ATI-SGR-PR/001.1:13

PSI – Termos e Definições Gerais

Versão 1.0

Válida a partir da publicação da Resolução 001/2013

Palavras-chave: Termos, Definições, Segurança, Informação, ATI.

Esse Documento é classificado como público

Agência Estadual de Tecnologia da Informação

14 páginas

Sumário

Prefácio

A Política de Segurança da Informação e seus documentos complementares utilizam diversos termos aos quais o usuário comum ou leigo poderá não estar acostumado. Para um melhor entendimento, e evitando replicações de termos e definições em diversos documentos, foi elaborado esse documento centralizado com todos os Termos e Definições Gerais, redigido 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].

1 Escopo

Essa Norma tem o objetivo de centralizar todos os termos e definições técnicos que serão utilizados em todo conjunto normativo de Segurança da Informação no âmbito da ATI.

2 Termos e Definições Gerais

Para os efeitos da Política de Segurança da Informação da ATI, que contempla o documento de Diretrizes Gerais e todos os demais documentos vinculados, aplicam-se os seguintes termos e definições:

2.1 Acesso Autorizado

Acesso previsto e permitido à informação, de forma direta ou indireta, e necessariamente decorrente do cumprimento da política de direito de acesso ou do mecanismo controle de acesso implementado vigentes.

2.2 Acesso Não Autorizado

Acesso indevido ou não previsto obtido, por quaisquer meios, procedimentos e a qualquer título, à revelia da política ou do controle de acesso vigentes, ou ainda decorrente de falhas ou imperfeições nos mecanismos de controle de acesso. Contrasta com acesso autorizado.

2.3 Ativos de Informação

O principal ativo de informação é a própria informação em si, mas esta definição também inclui qualquer hardware, software, sistemas, repositórios, mídias ou

dispositivos de qualquer natureza que gerem, manipulem, sirvam de meio de tráfego ou armazenem, ainda que temporariamente, dados ou informação próprias ou sob custódia.

2.4 Controle de Acesso

Mecanismo que implementa uma política restritiva de acesso a dados ou informações.

2.5 Custódia

Responsabilidade administrativa pessoal, setorial ou institucional pela guarda e proteção de ativos de informação de qualquer natureza, para a própria instituição ou para terceiros. Não implica, necessária e automaticamente, em direito de acesso à eventual informação que o ativo eventualmente contém.

2.6 Declaração de Aplicabilidade

Documento acessório específico que enumera exaustivamente e descreve os documentos relativos à Segurança da Informação (PSI e Documentos Acessórios). É recomendável que este documento discrimine, de forma exaustiva, a jurisdição e outros detalhes de cada um dos documentos, conforme o caso e necessidade.

2.7 Direito de Acesso

Privilégio associado e decorrente de processo, procedimento, cargo, função ou outra responsabilidade administrativa ou técnica formal, para o uso previamente autorizado de ativos de informação qualquer natureza.

2.8 Documentos Acessórios (Documentos Normativos Acessórios)

Qualquer documento formal e adicional ao documento da PSI, inspirado e construído a partir deste último, e que o interprete, regulamente, esclareça, oriente, explicite detalhes, complemente ou forneça qualquer subsídio adicional para o mapeamento e implementação das diretrizes da PSI na instituição, no seu todo ou em parte.

2.9 Doutrina (de Segurança da Informação)

Regras e boas práticas na Segurança da Informação, que são resultado da experiência acumulada pela comunidade de segurança na proteção da informação bem como da própria instituição, e que a torna uma diretriz de uso recomendável, exceto quando as condições ou situações específicas não indiquem inequivocamente o contrário. Apresenta-se sob a forma de elementos doutrinários utilizáveis no nível estratégico ou tático operacional (como códigos de prática e outras recomendações técnicas genéricas), constituindo importantes referências amplamente aplicáveis e aceitas.

2.10 Evento (de Segurança da Informação)

Ocorrência identificada, não importando os meios, que indica possível violação da PSI, falha de controles ou situação desconhecida, que possa ser relevante para a Segurança da Informação. Eventos requerem análise e conclusões.

2.11 Ferramentas (de Segurança da Informação)

Recursos de tecnologia, de qualquer natureza, que permitem algum nível de

sistematização ou automação nas tarefas de aplicação da PSI, normas ou procedimentos.

2.12 Incidente (de Segurança da Informação)

Evento ou ocorrência, acidental ou não, que denote ou implique impacto negativo, parcial ou total, na integridade, disponibilidade ou confidencialidade da informação.

2.13 Informação

Dados próprios ou custodiados que possuem sintaxe e semântica (pré ou pós) definidas, gerados, manipulados, em trânsito ou armazenados sob qualquer meio ou tecnologia, direta ou indiretamente pela instituição para o cumprimento de sua missão. Sua segurança é o principal ativo tutelado por esta Política de Segurança da Informação e seus documentos acessórios.

2.14 Norma (de Segurança da Informação)

Documento interno que regulamenta formal e administrativamente, de maneira geral ou específica, aspectos ou diretrizes expressas na PSI, no todo ou em parte da instituição. As normas mapeiam a PSI na organização técnico-administrativa da instituição, estabelecendo regras para a sua implementação.

2.15 Procedimento (de Segurança da Informação)

Documento interno e restrito que descreve ações ou rotinas técnico-administrativas consideradas praxe operacional, à luz das normas pertinentes.

2.16 PSI – Política de Segurança da Informação

A Política de Segurança da Informação, Política de Segurança ou simplesmente PSI, consiste na expressão pública e formal da ATI, no nível estratégico, no que concerne às suas preocupações com a segurança dos ativos de informação, no cumprimento de sua missão. A PSI é complementada/regulamentada por um conjunto de documentos acessórios, usualmente denotados por normas, procedimentos ou outros documentos, que a interpretam e a mapeiam na organização técnico-administrativa da instituição, sem prejuízo da submissão ao arcabouço legal vigente.

2.17 Responsabilidade

Obrigações e deveres decorrentes da legislação vigente, ofício, cargo, função ou por força de contrato, na proteção dos ativos de informação de qualquer natureza.

2.18 Responsáveis pela informação

Todo aquele que, por exigência legal, normativa, dever de ofício ou por força de contrato, tem como responsabilidade zelar pela implementação e manutenção, nos níveis requeridos, dos requisitos de confidencialidade, integridade e disponibilidade da informação nos termos deste documento.

2.19 Responsável pelo Setor

Ocupante de cargo ou função, ainda que interino ou em substituição, responsável pelas atribuições funcionais, bem como da aplicação da política, normas e procedimentos no âmbito do seu setor, área ou afim.

2.20 SGSI – Sistema de Gestão em Segurança da Informação

Instrumento interno de gestão, inspirado em sua concepção e tendo por referência a PSI e seus documentos acessórios, que deverá prover informações e oferecer os meios e oportunidades para um contínuo e efetivo acompanhamento e controle dos níveis de segurança requeridos pelos ativos de informação.

2.21 Segurança da Informação

Objetivo genérico da Política de Segurança e seu arcabouço normativo, a ser perseguido pelo diligente provimento às informações de níveis adequados de cada um dos pilares de privacidade, integridade e disponibilidade, como exige a necessidade e conforme recomenda a doutrina. As abordagens a serem utilizadas para a implementação de tais requisitos da informação são a prevenção, a detecção e a resposta adequadas a cada caso, e normalmente viabilizadas por uma combinação de tecnologias, pessoas e processos.

2.22 Senha ou Credencial de Acesso

Credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado ativo de informação de qualquer natureza, ou local que o abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes.

2.23 Setor Responsável

Setor, área ou afim associado por responsabilidade funcional, administrativa ou legal ao aspecto em questão.

2.24 System Hardening

Procedimentos efetuados em ativos de informação buscando encontrar um compromisso aceitável entre as funcionalidades necessárias, à Política de Segurança e normas vigentes, e os riscos inerentes ao seu funcionamento. Seu objetivo é prover o ativo de informação de algum nível de resistência própria às ameaças, de forma autônoma, e a despeito da existência de eventuais proteções externas adicionais.

2.25 Usuário (Usuário legítimo)

Todo aquele com acesso previsto e autorizado a um ativo de informação.

2.26 Usuário não autorizado (Usuário Ilegítimo)

Todo aquele que, por qualquer meio ou motivação, tenta ou se utiliza de ativos ou recursos da infraestrutura de tecnologia de forma imprópria, não autorizada ou não imprevista.

3 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, 2013. Disponível em: <www.ati.pe.gov.br>. Acesso em: 14 de mai. de 2013.