SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
GABINETE DO REITOR
Avenida Fernando Machado, 108-E, Centro, Chapecó-SC, CEP 89802-112, 49 2049-3700
gabinete@uffs.edu.br, www.uffs.edu.br

PORTARIA Nº 216/GR/UFFS/2018

O REITOR DA UNIVERSIDADE FEDERAL DA FRONTEIRA SUL (UFFS), no uso de suas atribuições legais, resolve:

TÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º ESTABELECER diretrizes, critérios, normas e procedimentos de Segurança da Informação e Comunicações no âmbito da Universidade Federal da Fronteira Sul (UFFS).

TÍTULO II
DO OBJETIVO E APLICAÇÃO

Art. 2º A Política de Segurança da Informação e Comunicações da Universidade Federal da Fronteira Sul (POSIC/UFFS) visa assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas e/ou custodiadas pela UFFS.

Art. 3º A Política é aplicada a todos que, direta ou indiretamente, possuem acesso às informações da Universidade Federal da Fronteira Sul (UFFS).

TÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para os efeitos desta Política, das normas complementares e dos procedimentos operacionais de Segurança da Informação e Comunicações criados no âmbito da UFFS, serão adotados os conceitos e as definições descritos no "Dicionário de Referência da POSIC/UFFS" (Anexo I).

TÍTULO IV
DOS PRINCÍPIOS E DA ABRANGÊNCIA

Art. 5º A POSIC/UFFS deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal (APF).

Art. 6º A Segurança da Informação e Comunicações da UFFS abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos seguintes princípios:
I - garantia da integridade, da autenticidade e da disponibilidade das informações;
II - proteção adequada das informações, de acordo com a necessidade de restrição de acesso;
III - planejamento das ações para manter a segurança da informação;
IV - transparência das informações públicas, de acordo com a legislação vigente.

CAPÍTULO I
DOS ATIVOS DE INFORMAÇÃO

Art. 7º Os ativos de informação da UFFS devem ser inventariados e atribuídos a gestores e custodiantes.

Art. 8º Todos os sistemas de informação da UFFS, automatizados ou não, devem ter um gestor do ativo de informação, formalmente designado pela autoridade competente.

CAPÍTULO II
DO TRATAMENTO DA INFORMAÇÃO

Art. 9º Toda informação deve ser protegida no acesso, tráfego, uso, armazenamento e descarte, de acordo com sua classificação em graus de sigilo à UFFS, ao Estado e às pessoas.
Parágrafo único: o termo "protegida" referido no caput significa preservar a integridade, a confidencialidade, a disponibilidade, a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela Universidade.

CAPÍTULO III
DO CONTROLE DE ACESSO

Art. 10 O controle de acesso observará as diretrizes e normas complementares desta Política, as recomendações e as alterações da NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSIPR de 15/07/2014 do Gabinete de Segurança Institucional da Presidência da República, da INSTRUÇÃO NORMATIVA CONJUNTA CGU/MO001 DE 10/05/2016 e da ABNT NBR ISO/IEC 27002:2013.

Art. 11 Todos os usuários são responsáveis pelos ativos de informação e comunicações aos quais têm acesso, bem como por utilizá-los estritamente dentro do propósito institucional, sendo vedado seu uso para fins particulares ou de terceiros.

Art. 12 A concessão de acesso deve ser realizada em conformidade com o princípio do privilégio mínimo, ou seja, cada credencial de acesso deve possuir apenas o conjunto de privilégios estritamente necessários ao desempenho das suas atribuições profissionais.
§ 1º As tentativas de autenticação, concessão e revogação de privilégios de acesso, em qualquer ativo de tecnologia da informação, devem ser registradas de modo que seja possível determinar a data e hora na qual ocorreram, os identificadores de acesso utilizados e o ativo de informação-alvo, bem como os privilégios concedidos e revogados.
§ 2º Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuídos.

Art. 13 O ativo arquivístico digital de longa temporalidade ou de caráter permanente produzido pelo usuário deverá ser mantido em Repositório Arquivístico Digital Confiável (RDC-Arq), em conformidade com a legislação vigente.

Art. 14 Os espaços físicos de atuação da UFFS devem ser adequadamente protegidos, visando salvaguardar os ativos de informação, conforme a classificação de risco de cada ambiente.

CAPÍTULO IV
DO USO DE CORREIO ELETRÔNICO, DA INTERNET E DAS REDES SOCIAIS

Art. 15 O uso da Internet, de *e-mail* corporativo e das redes sociais, no âmbito da UFFS, devem ser detalhados em normas específicas em conformidade com as diretrizes desta Política.

Parágrafo único: Diretrizes para Gestão Arquivística devem ser observadas através da Resolução Nº 36 do Conselho Nacional de Arquivos (CONARQ) e legislação em vigência.

CAPÍTULO V
DA AUDITORIA E CONFORMIDADE

Art. 16 O uso dos recursos computacionais e de informações da UFFS é passível de monitoramento, respeitando-se os princípios da legislação vigente.
Parágrafo único. Mecanismos que permitam a rastreabilidade desse uso devem ser detalhados em normas específicas em conformidade com as diretrizes desta Política.

Art. 17 As condições e os termos de licenciamento de *software* e os direitos de propriedade intelectual devem ser, obrigatoriamente, respeitados.
Parágrafo único. Somente é permitida a instalação de programas (*software*) em ativos de tecnologia da informação da UFFS, independentemente do regime de licenciamento, para o cumprimento de atividades de interesse institucional.

CAPÍTULO VI
DA GESTÃO DA CONTINUIDADE

Art. 18 A UFFS deve elaborar, implementar e instituir processos e normas que estabeleçam a Gestão de Continuidade do Negócio.
Parágrafo único. A UFFS deverá dispor de processos que assegurem a disponibilidade e a integridade dos ativos de informação.

CAPÍTULO VII
DOS CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Art. 19 Todos os contratos, convênios, acordos e instrumentos congêneres devem:
I - Conter cláusulas que estabeleçam a obrigatoriedade de observância e aceitação desta Política de Segurança de Informação e Comunicações e de suas normas complementares.
II - A instalação, a compra e o uso de soluções que envolvam a informação e a comunicação devem atender à legislação vigente.
III - Nos instrumentos indicados no caput, devem constar cláusulas de confidencialidade, bem como cláusulas que determinem as sanções cabíveis em caso de descumprimento desta Política.

CAPÍTULO VIII
DA GESTÃO DE RISCOS

Art. 20 A UFFS implementará e manterá processos de gestão de riscos para prevenir e tratar incidentes e proteger os ativos de informação e comunicações.
Parágrafo único. Os processos devem possibilitar a classificação de ordem de prioridade dos ativos e a definição e implementação de controles para identificação e tratamento de problemas de segurança.

Art. 21 A UFFS instituirá e manterá a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

Art. 22 Devem ser instituídas metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança da informação e comunicações.

CAPÍTULO IX
DA PUBLICIDADE E CAPACITAÇÃO

Art. 23 A POSIC/UFFS deve ser conhecida e seguida por todos os usuários do órgão, sendo difundida na UFFS por meio de um processo permanente de conscientização e sensibilização em Segurança da Informação e Comunicações.

Art. 24 A UFFS deverá prover, regularmente, capacitação especializada em Segurança da Informação e Comunicações aos membros da ETIR, a fim de garantir a adequada gestão, manutenção destas diretrizes e tratamento de incidentes, como recomendam as Normas Complementares Nº 08/IN01/DSIC/GSIPR, Nº 17/IN01/DSIC/GSIPR e Nº 18/IN01/DSIC/GSIPR do Gabinete de Segurança Institucional da Presidência da República.

TÍTULO V
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 25 Todos os agentes públicos que necessitem acesso às informações devem assinar, antes do início de suas atribuições, termo de responsabilidade e confidencialidade, garantindo o conhecimento e zelo pelo adequado cumprimento desta Política de Segurança da Informação e Comunicações.

Art. 26 Ao Reitor, de acordo com a Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008, compete:
I - Coordenar as ações de Segurança da Informação e Comunicações;
II - Aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;
III - Propor programa orçamentário específico para as ações de Segurança da Informação e Comunicações;
IV - Nomear Gestor de Segurança da Informação e Comunicações;
V - Instituir e implementar Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
VI - Instituir Comitê de Segurança da Informação e Comunicações;
VII - Aprovar Política de Segurança da Informação e Comunicações e demais normas de Segurança da Informação e Comunicações;
VIII - Remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações, sempre que solicitado formalmente, ao GSI/PR.
IX - Prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR e do Comitê de Segurança da Informação e Comunicações, bem como prover a infraestrutura necessária.

Art. 27 Aos membros do Comitê de Segurança da Informação e Comunicações da UFFS, de acordo com a Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008, compete:
I - Assessorar a Administração da UFFS na implementação das ações de Segurança da Informação e Comunicações;

II - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação e Comunicações;
III - Propor alterações na Política de Segurança da Informação e Comunicações;
IV - Propor normas e procedimentos internos relativos à Segurança da Informação e Comunicações, em conformidade com as legislações existentes sobre o tema.

Art. 28 Ao Gestor de Segurança da Informação e Comunicações, de acordo com a Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008, compete:
a) Promover a cultura de Segurança da Informação e Comunicações no âmbito da UFFS;
I - Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
II - Propor recursos necessários às ações de Segurança da Informação e Comunicações;
III - Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
IV - Realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na Segurança da Informação e Comunicações;
V - Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à Segurança da Informação e Comunicações;
VI - Propor normas e procedimentos relativos à Segurança da Informação e Comunicações no âmbito do UFFS.

Art. 29 À Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais compete, em consonância com as Normas Complementares Nº 05/IN01/DSIC/GSIPR e Nº 08/IN01/DSIC/GSIPR do Gabinete de Segurança Institucional da Presidência da República:
I - Receber, analisar e responder a notificações e atividades relacionadas aos incidentes de Segurança da Informação e Comunicações;
II - Registrar todos os incidentes notificados ou detectados, com a finalidade de assegurar registro histórico das atividades da ETIR.

TÍTULO VI
DAS PENALIDADES
CAPÍTULO I
DAS SANÇÕES E PENALIDADES

Art. 30 Em caso de descumprimento de termos estabelecidos nesta Portaria, serão aplicadas as sanções e penalidades previstas na legislação vigente e nas regulamentações internas da UFFS.

Art. 31 Em casos de risco ou quebra de Segurança da Informação e Comunicações por meios eletrônicos, o Gestor de CSIC e a ETIR devem ser imediatamente acionados para adotar as providências necessárias, podendo inclusive determinar a restrição temporária do acesso às informações e/ou aos recursos computacionais da UFFS.

TÍTULO VII
DISPOSIÇÕES FINAIS

Art. 32 Os casos omissos serão analisados e deliberados pelo Comitê de Segurança da Informação e Comunicações da UFFS.

Art. 33 Os Instrumentos normativos gerados a partir da POSIC/UFFS, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

Art. 34 Demais requisitos de segurança, normas, procedimentos da Segurança da Informação e Comunicações serão estabelecidos em normas complementares específicas a esta Política.

TÍTULO VIII
DA VIGÊNCIA

Art. 35 Esta Portaria entra em vigor a partir de sua publicação no Boletim Oficial da UFFS.

Chapecó-SC, 9 de março de 2018.

JAIME GIOLO
Reitor

ANEXO I

DICIONÁRIO DE REFERÊNCIA DA POSIC-UFFS

ABREVIATURAS

APF: Administração Pública Federal.
ETIR: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.
Gestor de SIC: Gestor de Segurança da Informação e Comunicações.
GSI/PR: Gabinete de Segurança Institucional da Presidência da República.
POSIC-UFFS: Política de Segurança da Informação e Comunicações da Universidade Federal da Fronteira Sul-UFFS.
POSIC: Política de Segurança da Informação e Comunicações.
SIC: Segurança da Informação e Comunicações.

CONCEITOS E DEFINIÇÕES

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.
Fonte: NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSIPR.

Agente público: aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta.
Fonte: NORMA COMPLEMENTAR Nº 18/IN01/DSIC/GSIPR.

Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportam um ou mais produtos ou serviços.
Fonte: NORMA COMPLEMENTAR Nº 06/IN01/DSIC/GSIPR.

Ativos de Informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como locais onde se encontram esses meios e as pessoas que a eles têm acesso.
Fonte: NORMA COMPLEMENTAR Nº 04/IN01/DSIC/GSI/PR.

Autenticidade: garantia de que a informação foi produzida, expedida, modificada ou destruída por determinada pessoa física ou determinado sistema, órgão ou entidade.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.

Capacitação: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores do tema, estando aptos para atuar em suas organizações como gestores de SIC.
Fonte: NORMA COMPLEMENTAR Nº 18/IN01/DSIC/GSIPR.

Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.
Fonte: NORMA COMPLEMENTAR Nº 03/IN01/DSIC/GSIPR.

Confidencialidade: garantia de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.

Conformidade: cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização.
Fonte: NORMA COMPLEMENTAR Nº 11/IN01/DSIC/GSIPR.
Conscientização: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores do tema.
Fonte: NORMA COMPLEMENTAR Nº 18/IN01/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.
Fonte: NORMA COMPLEMENTAR Nº 06/IN01/DSIC/GSIPR.
Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.
Fonte: NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSIPR.
Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo, ou lógica, como identificação de usuário e senha.
Fonte: NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSIPR.
Custodiante do ativo de informação: 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.
Fonte: NORMA COMPLEMENTAR Nº 10/IN01/DSIC/GSIPR.
Disponibilidade: garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.
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.
Fonte: NORMA COMPLEMENTAR Nº 05/IN01/DSIC/GSIPR.
Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso tais ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado.
Fonte: NORMA COMPLEMENTAR Nº 06/IN01/DSIC/GSIPR.
Gestão de riscos de segurança da informação e comunicações: conjunto de 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 equilibrá-los com os custos operacionais e financeiros envolvidos.
Fonte: NORMA COMPLEMENTAR Nº 04/IN01/DSIC/GSI/PR.

Gestão de segurança da informação e comunicações: ações e métodos que visam a 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.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.

Gestor de segurança da informação e comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.
Fonte: NORMA COMPLEMENTAR Nº 03/IN01/DSIC/GSIPR.

Gestão da continuidade de negócios: processo contínuo de gestão e governança suportado pela alta direção que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção.
Fonte: NORMA COMPLEMENTAR Nº 06/IN01/DSIC/GSIPR.

Gestor do ativo de informação: refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, que é responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumindo, no mínimo, as seguintes atividades:
a) descrever o ativo de informação;
b) definir as exigências de segurança da informação e comunicações do ativo de informação;
c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;
d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento;
e) indicar os riscos que podem afetar os ativos de informação.
Fonte: NORMA COMPLEMENTAR Nº 10/IN01/DSIC/GSIPR.

Identificação e classificação de ativos de informação - processo composto por 6 (seis) etapas:
a) coletar informações gerais;
b) definir as informações dos ativos;
c) identificar o(s) responsável(is);
d) identificar os contêineres dos ativos;
e) definir os requisitos de segurança;
f) estabelecer o valor do ativo de informação.
Fonte: NORMA COMPLEMENTAR Nº 10/IN01/DSIC/GSIPR.

Incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
Fonte: NORMA COMPLEMENTAR Nº 05/IN01/DSIC/GSIPR.

Incidente: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
Fonte: NORMA COMPLEMENTAR Nº 06/IN01/DSIC/GSIPR.
Integridade: garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.
Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suportes administrativos suficientes à implementação da segurança da informação e comunicações.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.
Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.
Redes sociais: estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.
Fonte: NORMA COMPLEMENTAR Nº 15/IN01/DSIC/GSIPR.
Requisitos de segurança: conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança, como controle de acesso baseado em papéis de usuários (administradores, usuários comuns, etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais, etc.), dentre outros. Os aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense.
Fonte: NORMA COMPLEMENTAR Nº 16/IN01/DSIC/GSIPR.
Segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.
Sensibilização: atividade de ensino que tem como objetivo orientar sobre o que é Segurança da Informação e Comunicações (SIC), fazendo com que os participantes possam perceber em sua rotina pessoal e profissional ações que precisam ser corrigidas.
Fonte: NORMA COMPLEMENTAR Nº 18/IN01/DSIC/GSIPR.
Termo de responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.
Fonte: NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSIPR.
Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Fonte: INSTRUÇÃO NORMATIVA GSI/PR N. 1, DE 13 DE JUNHO DE 2008.

Tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

Fonte: NORMA COMPLEMENTAR Nº 05/IN01/DSIC/GSIPR.

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.

Fonte: NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSIPR.