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

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.