Prefeitura Municipal de
Angra dos Reis

PREFEITURA Angra | angra prev

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

(PSIC)

Agosto/2025

Prefeitura Municipal de
Angra dos Reis

PREFEITURA Angra | angra prev

IDENTIFICAÇÃO

RAZÃO SOCIAL: Instituto de Previdência Social do Município de Angra dos Reis		
CNPJ: 10.590.600/0001-00	**DATA DE CRIAÇÃO:** 29/12/2008	
NATUREZA JURÍDICA: Entidade Autárquica de Direito Público		
ENDEREÇO: Rua Doutor Orlando Gonçalves nº 231 – Parque das Palmeiras		
CIDADE: Angra dos Reis	**ESTADO:** Rio de Janeiro	**CEP:** 23.906-540
TELEFONE: (24) 3365-5388		

DIRETORIA EXECUTIVA

Diretor-Presidente
Carlos Renato Pereira Gonçalves

Controladora Interna
Giovanna Martins Valladão Soares

Diretora de Administração
Edenilze Alves Ferreira Dias

Diretor Financeiro
Victor Hugo Pereira de Abreu

Diretor de Benefícios
Pedro Cauisa da Cunha Miguel Souza

Diretora de Recursos Humanos
Mayara do Nascimento Rosa

Diretor de Contabilidade
Fernando de Moraes Ribeiro

Histórico de Revisões (versionamento)

Data	Versão	Descrição	Unidade
14/08/2020	1.0	Publicada em Boletim Oficial nº 1356 - 08 de Julho de 2021	
15/08/2025	2.0	Versão aprovada em reunião de diretoria executiva em 15/08/2025, em reunião de Conselho Deliberativo em 26/08/2025.	

Sumário

1. OBJETIVO

Esta Política de Segurança da Informação e Comunicação (PSIC) tem como objetivo estabelecer diretrizes para garantir confidencialidade, integridade e disponibilidade das informações do Instituto de Previdência Social de Angra dos Reis – ANGRAPREV, assegurando a proteção dos ativos de informação contra ameaças internas e externas.

Desse modo, esta PSIC busca preservar os ativos de informação, assim como a imagem institucional do ANGRAPREV, orientando procedimentos adequados para manuseio, tratamento, controle, divulgação e proteção dos dados, informações e documentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso do Instituto.

O propósito desta PSIC é orientar o ANGRAPREV quanto à gestão de riscos e ao tratamento de incidentes de segurança da informação e comunicação, em conformidade com as disposições constitucionais, legais e regimentais vigentes.

2. ESCOPO

Esta PSIC estabelece o comprometimento da alta diretoria organizacional do ANGRAPREV, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança da Informação e Comunicação (GRSIC).

As diretrizes de segurança da informação estabelecidas nesta PSIC aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo ANGRAPREV, e todos os usuários são responsáveis por sua aplicação e comprometidos com os princípios estabelecidos.

É responsabilidade de todas as Diretorias/Áreas dar amplo conhecimento do teor desta PSIC, sendo todos considerados responsáveis por garantir a segurança das informações a que tenham acesso.

2.1. Abrangência

Esta PSIC se aplica à Sede do ANGRAPREV abrangendo todos servidores públicos, colaboradores internos ou externos, prestadores de serviços, parceiros e qualquer outra parte que tenha acesso às informações e aos recursos de tecnologia da informação do ANGRAPREV, incluindo sistemas, redes, dados, aplicativos, dispositivos e processos relacionados ao uso da informação, inclusive quando da utilização de equipamentos pessoais.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

3. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Esta PSIC e as ações dela derivadas baseiam-se nos seguintes princípios fundamentais:

Confidencialidade: garantir que a informação seja acessível apenas a pessoas autorizadas.

Integridade: assegurar a exatidão e a completude das informações, livres de alterações indevidas, garantindo a precisão e confiabilidade dos dados armazenados e transmitidos.

Disponibilidade: assegurar que os usuários autorizados tenham acesso à informação e aos ativos associados sempre que necessário.

Ética: preservar os direitos e interesses legítimos de usuários e agentes públicos, promovendo um ambiente confiável.

Proporcionalidade: assegurar medidas de segurança proporcionais aos riscos identificados, evitando excessos que possam comprometer a eficiência das operações.

Celeridade: priorizar respostas rápidas e eficazes a incidentes, falhas de segurança e necessidades operacionais, minimizando impactos.

Legalidade: observar estritamente a legislação vigente, normas internas e políticas organizacionais, respeitando as atribuições regimentais do ANGRAPREV.

Publicidade: garantir a transparência na gestão e comunicação de informações, observados os critérios de confidencialidade, integridade e disponibilidade, conforme estabelecido por lei.

4. COMPETÊNCIAS E RESPONSABILIDADES

4.1. Diretoria Executiva do ANGRAPREV

a) Apoiar a promoção da cultura de segurança da informação e comunicação;

b) Aprovar a PSIC;

c) Avaliar o orçamento para ações de segurança da informação e comunicação proposto pelo Comitê Gestor de Segurança da Informação e Comunicação (CGSIC).

4.2. Presidência do ANGRAPREV

a) Apoiar a promoção da cultura de segurança da informação e comunicação;

b) Nomear o comitê Gestor de Segurança da Informação e Comunicação (GSIC);

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

c) Aplicar ações corretivas e disciplinares cabíveis em casos de quebra de segurança e violações desta PSIC;

d) Aprovar o orçamento para ações de segurança da informação e comunicação, conforme proposto pelo Comitê Gestor de Segurança da Informação e Comunicação (CGSIC).

4.3. Gestor de Segurança da Informação e Comunicação (GSIC)

a) Difundir a cultura de segurança da informação e comunicação;

b) Coordenar a elaboração e implementação da PSIC;

c) Coordenar o Comitê Gestor de Segurança (CGSIC) e a Equipe de Resposta a Incidentes (ETIR);

d) Coordenar as ações de segurança da informação e comunicação e propor recursos necessários;

e) Acompanhar investigações e avaliações dos danos decorrentes de quebras de segurança e submeter relatórios consolidados à Presidência do ANGRAPREV, após análise do CGSIC;

f) Realizar estudos sobre novas tecnologias e seus impactos na segurança da informação e comunicação;

g) Propor normas e procedimentos relativos à segurança da informação e comunicação;

h) Propor meios para capacitar a equipe da ETIR e para assegurar sua infraestrutura;

i) Divulgar internamente esta PSIC.

4.4. Comitê Gestor de Segurança da Informação e Comunicações (CGSIC)

a) Promover a cultura de segurança da informação e comunicação;

b) Implementar, monitorar, avaliar e propor alterações nesta PSIC e suas normas;

c) Propor normas e procedimentos de segurança da informação e comunicação em conformidade com legislações vigentes;

d) Assessorar a implementação das ações de segurança da informação e comunicação do ANGRAPREV;

e) Propor à Presidência do Instituto penalidades em caso de violações desta PSIC;

f) Formar grupos de trabalho para soluções específicas;

g) Solicitar investigações em casos suspeitos de quebra de segurança;

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

h) Avaliar, revisar e analisar a PSIC e normas complementares, visando garantir sua aderência às legislações e objetivos institucionais;

i) Dirimir dúvidas e deliberar questões relacionadas à PSIC;

j) Propor Plano de Investimentos em segurança da informação e comunicação;

k) Propor programa orçamentário específico para ações em segurança da informação e comunicação;

l) Definir e atualizar seu Regimento Interno.

4.5. Equipe de tratamento de incidentes em redes de computadores (ETIR)

a) Coordenar e facilitar atividades de tratamento e resposta a incidentes de segurança da informação e comunicação;

b) Recuperar sistemas afetados;

c) Atuar proativamente, promovendo boas práticas e verificações de segurança nas redes;

d) Responder reativamente a incidentes, orientando no reparo e na análise de sistemas comprometidos, avaliando causas e responsáveis;

e) Investigar ataques e intrusões na rede do ANGRAPREV;

f) Executar ações necessárias para tratar violações de segurança;

g) Coletar dados quantitativos de incidentes (natureza, causa, data, frequência, custos);

h) Participar de fóruns e redes relacionadas à segurança da informação e comunicação.

4.6. Proprietário de ativos de informação

a) Descrever os ativos de informação e administrar seus requisitos de segurança sob sua responsabilidade;

b) Monitorar continuamente a segurança dos ativos sob sua responsabilidade;

c) Comunicar as exigências de segurança da informação e comunicação a usuários e custodiantes;

d) Gerenciar acessos (concessão e revogação) aos ativos de informação;

e) Relatar riscos e incidentes à ETIR;

f) Designar custodiante para os ativos, quando aplicável.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

4.7. Custodiante dos ativos de informação

a) Proteger e manter os ativos de informação;

b) Controlar acessos de acordo com os requisitos do proprietário da informação e a PSIC;

c) Definir e gerir os requisitos de segurança dos ativos sob sua responsabilidade.

4.8. Usuários dos ativos de informação

a) Conhecer e cumprir os princípios, diretrizes e responsabilidades da PSIC, bem como normativos e resoluções relacionados;

b) Seguir os requisitos de controle definidos pelos gestores e custodiantes da informação;

c) Reportar incidentes de segurança dos ativos à ouvidoria ou à ETIR.

4.9. Prestadores de serviço, fornecedores e colaboradores externos

a) Conhecer e cumprir a PSIC;

b) Fornecer listas atualizadas de documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;

c) Disponibilizar toda a documentação de sistemas, produtos e serviços relacionados às atividades prestadas.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas, sem prejuízo da Legislação vigente, conforme seu nível de sensibilidade:

Pública: Pode ser divulgada sem restrições.

Interna: Uso restrito a colaboradores.

Confidencial: Acesso limitado a grupos específicos.

Sigilosa: Informações críticas cujo vazamento pode causar danos graves.

Cada nível de classificação requer cuidados específicos em seu armazenamento, transmissão e descarte.

6. DIRETRIZES GERAIS

Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo ANGRAPREV serão utilizados exclusivamente para fins institucionais, e em

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

conformidade com esta PSIC, bem como com suas normas internas e legislação vigente. É premissa não comprometer a integridade, a confidencialidade, a confiabilidade, a autenticidade e a disponibilidade da informação independentemente da forma ou do meio pelo qual seja apresentada ou compartilhada, devendo esta ser sempre protegida adequadamente, de acordo com esta PSIC.

É vedada a utilização dos recursos de TIC do ANGRAPREV para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar leis, regulamentos, direitos autorais ou comprometer a moral e a ética institucional.

As diretrizes desta PSIC estabelecem os pilares fundamentais da Gestão de Segurança da Informação e Comunicação, orientando a criação e atualização das normas internas. Os casos omissos e as dúvidas decorrentes da aplicação do disposto nesta PSIC devem ser encaminhados ao Comitê Gestor de Segurança da Informação e Comunicações (CGSIC).

7. DIRETRIZES ESPECÍFICAS

7.1. Gestão da Segurança da Informação e Comunicação

Todos os mecanismos e controles de proteção voltados para a Segurança da Informação e Comunicação devem ser mantidos com o objetivo de assegurar a continuidade das atividades do ANGRAPREV e a proteção de seus ativos.

As medidas de proteção devem ser adequadamente planejadas, considerando que os gastos para implementação de controles sejam compatíveis com o valor do ativo protegido.

Os requisitos de segurança da informação e comunicação do ANGRAPREV devem ser citados nos termos de compromisso celebrados com terceiros. Esses documentos devem incluir cláusulas que determinem a obrigatoriedade de atendimento e divulgação das diretrizes desta PSIC aos seus colaboradores, bem como a responsabilização no caso de descumprimento, devendo ainda ser exigido, quando necessário, um termo de confidencialidade e um plano de mitigação de riscos específico.

7.2. Gestão de Riscos e Segurança da Informação e Comunicação – GRSIC

É um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação do ANGRAPREV, equilibrando-os de forma proporcional com os custos operacionais, financeiros e impactos potenciais envolvidos.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

As áreas responsáveis por ativos de informação deverão manter processos contínuos de Gestão de Riscos, que serão aplicados na implementação, operação e monitoramento da GRSIC.

A GRSIC no âmbito do ANGRAPREV deverá:

- Identificar e classificar os ativos de informação conforme sua criticidade e relevância;
- Determinar ações de gestão apropriadas, priorizando a mitigação dos riscos mais críticos;
- Estabelecer controles preventivos e corretivos, além de planos de contingência para reduzir vulnerabilidades identificadas.

A GRSIC deverá ser avaliada quanto à necessidade de alterações uma vez ao ano, ou nos casos de mudanças organizacionais, surgimento de novas ameaças ou identificação de vulnerabilidades.

Como parte integrante do programa de Gestão de Riscos, a GRSIC deverá incluir:

• **Plano de Continuidade de Negócios (PCN):** Deve complementar a análise de riscos, limitando os impactos de incidentes e garantindo que as informações e os recursos críticos para os processos de negócio estejam prontamente disponíveis, minimizando interrupções.

• **Plano de Gerenciamento de Incidentes (PGI):** Deve definir responsabilidades claras, procedimentos detalhados e critérios para assegurar respostas rápidas, efetivas e ordenadas perante incidentes relacionados à SIC, com foco em reduzir impactos e prevenir recorrências.

7.3. Gestão de Incidentes de Segurança (GIS)

Todos os eventos e incidentes de Segurança da Informação e Comunicação (SIC) devem ser imediatamente reportados ao setor de TI para que sejam registrados, investigados e tratados de forma sistemática com base em um plano de resposta e recuperação.

O Setor de TI deverá:

a) Receber as notificações de incidentes, analisar e avaliar o impacto;

b) Identificar causas e responder todas as notificações relacionadas à incidentes de segurança em redes de computadores;

c) Propor e implementar medidas preventivas ou corretivas para mitigar riscos futuros.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

7.4. Gestão de Continuidade de Negócios (GECON)

É um processo que busca aprimorar a resiliência organizacional, identificando ameaças potenciais aos ativos de informação e seus possíveis impactos nas operações, garantindo respostas eficazes a incidentes de SIC e minimizando impactos decorrentes de falhas, desastres ou indisponibilidades, além de recuperar ativos de informação perdidos.

As diretorias do ANGRAPREV devem, de forma pró-ativa, mapear e informar quais dos seus processos e recursos (equipamento e softwares) necessitam de medidas de respostas à interrupções, incidentes e sinistros, com vistas à elaboração de estratégias e procedimentos para lidar com situações que comprometam a continuidade de serviços. Essas estratégias devem assegurar a disponibilidade dos ativos de informação e a recuperação de atividades críticas, mitigando o impacto de eventos inesperados até a retomada da normalidade.

7.5. Controle de Acesso e Uso de Senha

O acesso às informações deve ser concedido com base no princípio do menor privilégio, e devem ser revisadas periodicamente.

O acesso deve ser revogado imediatamente em caso de desligamento ou encerramento de contrato, e deve ser revisto imediatamente em caso de mudança de função.

As autenticações de acesso devem utilizar senhas fortes e, quando disponível, múltiplos fatores de autenticação.

O acesso a sistemas, intranet, internet, informações, dados e instalações físicas do ANGRAPREV deve obedecer regulamentos e normas internas com o objetivo de garantir a segurança dos usuários e a proteção dos ativos institucionais.

As senhas de acesso são estritamente pessoais e intransferíveis, não devendo ser compartilhadas nem anotadas de modo que possam ser utilizadas por terceiros.

7.6. Acesso e utilização de Internet, E-mail e Redes Sociais

A utilização da internet, e-mails e redes sociais no ambiente do ANGRAPREV, para quaisquer finalidades, deve seguir normas e procedimentos específicos, atender à legislação vigente, às determinações desta PSIC e demais orientações governamentais, seja o acesso feito através dos computadores institucionais ou de ponto de acesso Wi-fi.

A gestão de perfis institucionais em redes sociais deve alinhar-se a esta PSIC e aos objetivos estratégicos do ANGRAPREV para prestação de serviços, atendimento ao público e compartilhamento de informações.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

7.7. Uso de computação em nuvem

A utilização de computação em nuvem para demandas de transferência e armazenamento de documentos, inteligência artificial e processamento de dados, aplicações, sistemas e demais tecnologias deve garantir, primordialmente, a confidencialidade dos dados, bem como a disponibilidade, integridade e autenticidade das informações, atendendo esta PSIC, normas específicas e demais orientações governamentais e legislação em vigor.

7.8. Uso de dispositivos móveis e equipamentos particulares

O uso de dispositivos móveis e outros equipamentos, sobretudo os particulares, para acessar informações e sistemas do ANGRAPREV deve ser previamente autorizado pelo setor de TI e seguir normas específicas que priorizem segurança das informações e requisitos legais.

7.9. Segurança de equipamentos, dispositivos e de redes e comunicações

Os equipamentos e dispositivos próprios do ANGRAPREV devem ser devidamente identificados e patrimoniados, e assegurada sua proteção contra uso indevido, perda ou roubo. Estes equipamentos devem utilizar a rede corporativa, bem como seu domínio de rede.

A disponibilização de acesso à internet para visitantes e atividades particulares deve se dar por rede independente e não conectada à rede corporativa.

É terminantemente proibida, sem prévia autorização do setor de TI do ANGRAPREV, a instalação de equipamentos e dispositivos que não sejam de propriedade do ANGRAPREV, bem como a instalação de softwares, ainda que sejam gratuitos e/ou de código livre.

7.10. Segurança física e ambiental

O acesso físico aos ambientes de TI (servidores, roteadores etc) deve ser restrito e controlado, os equipamentos devem estar protegidos contra riscos ambientais, e os visitantes e prestadores de serviço devem ser autorizados previamente e acompanhados durante os acessos.

7.11. Conformidade legal e normativa

O ANGRAPREV compromete-se a cumprir a legislação aplicável, bem como a Lei Geral de Proteção de Dados (LGPD) e normas de mercado.

Serão realizadas periodicamente auditorias internas para verificar a conformidade das normas e procedimentos desta PSIC ou derivados dela.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

7.12. Monitoramento, Auditoria e conformidade

O monitoramento, auditoria e conformidade observarão as seguintes diretrizes:

a) O uso de recursos tecnológicos é passível de monitoramento e auditoria, com mecanismos de rastreabilidade implementados quando for possível;

b) A movimentação de equipamentos e ativos de informação do ANGRAPREV deverão ser registrados e autorizados formalmente por autoridade competente e comunicados ao setor de TI;

c) Deverão ser mantidos registros e procedimentos, e quando possível, trilhas de auditoria que assegurem rastreamento, acompanhamento e controle de acessos aos sistemas institucionais, rede interna e internet;

d) Denúncias relacionadas a esta PSIC deverão ser encaminhadas ao setor de TI ou à Ouvidoria do ANGRAPREV.

7.13. Procedimentos Operacionais

O setor de TI formalizará procedimentos técnicos operacionais em documentos privados para casos específicos (backup, acesso lógico etc), de modo a não expor informações técnicas críticas que possam ser exploradas de forma indevida.

7.14. Conscientização, sensibilização e capacitação

O ANGRAPREV deverá garantir a divulgação interna da PSIC e normas derivadas, indicar cursos e promover a participação em programas contínuos de capacitação, reciclagem e aperfeiçoamento, bem como promover e incentivar uma cultura de segurança institucional por meio de campanhas internas, seminários e divulgação na sua rede interna, de forma a conscientizar os usuários.

7.15. Penalidades e sanções

A violação desta PSIC, bem como de diretrizes, normas e procedimentos dela derivados será devidamente apurada, podendo resultar aos responsáveis penalidades estabelecidas pela Presidência do ANGRAPREV, sem prejuízo de encaminhamento à Comissão de Ética e outras sanções administrativas, civis e penais, quando aplicáveis.

7.16. Revisão da política (atualização e validade)

Esta PSIC tem validade indeterminada, ou seja, permanecerá vigente até que outro marco normativo a atualize ou revogue, e será revisada sempre que ocorrerem mudanças significativas nos processos, diretrizes governamentais e na legislação aplicável. Para garantir o contínuo aperfeiçoamento deverão ser documentadas as lições aprendidas na aplicação desta PSIC.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

As atualizações desta PSIC e de seus normativos relacionados devem ocorrer conforme os seguintes critérios:

Política de Segurança da Informação e Comunicação (PSIC)

a) Nível de aprovação: Diretoria Executiva e Conselho Deliberativo (Conselho Administrativo – CONSAD).

b) Periodicidade de revisão: Anual.

Normas de Segurança da Informação

a) Nível de aprovação: Comitê de Segurança da Informação e Comunicações (CGSIC).

b) Periodicidade de revisão: Semestral.

Procedimentos Operacionais

a) Nível de aprovação: Área Técnica.

b) Periodicidade de revisão: Semestral.

Gestão de riscos e segurança da informação e comunicação (GRSIC)

A GRSIC deverá ser atualizada periodicamente, no mínimo uma vez por ano ou, quando necessário, em função de inventários de ativos, mudanças organizacionais, surgimento de novas ameaças ou identificação de vulnerabilidades. Essa atualização deve ser formalmente documentada.

8. CONCEITOS E DEFINIÇÕES

Para os efeitos desta PSIC, e dos documentos dela derivados, são estabelecidos os seguintes conceitos e definições:

Acesso: ato de ingressar, transitar, conhecer ou consultar informações, sistemas, dados, bem como aos ativos de informação.

Ameaça: qualquer evento que explore vulnerabilidades, ou seja, causa potencial de um incidente, que pode resultar em dano para um sistema ou organização.

Análise de Riscos: uso sistemático de informações para identificar, analisar e avaliar fontes de riscos.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços.

Ativo: qualquer componente (seja humano, tecnológico, software ou outros) que sustente.

Ativos de Informação: os meios de armazenamento, transmissão e processamento; os sistemas de informação; além das informações em si, bem como os locais em que se encontram esses meios e as pessoas que têm acesso a eles.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Avaliação de Riscos: processo de comparar o risco estimado com critérios predefinidos para determinar a importância do risco.

Classificação da Informação: identificação dos níveis de proteção que as informações demandam; atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas.

Comunicação do Risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado ou não credenciado.

Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

Custodiante do Ativo de Informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos em sua capacidade de prestar serviços essenciais ou críticos, por um período superior ao prazo de recuperação.

Descarte: eliminação correta de informações, documentos, mídias e acervos digitais.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

Estimativa de Riscos: processo utilizado para atribuir valores à probabilidade e consequências de determinado risco.

Eficácia: realização de um trabalho que atinja os resultados esperados.

Eficiência: realização de um trabalho, com presteza, agilidade e eficácia.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

Ética: preservação dos direitos dos agentes públicos, sem comprometimento da Segurança da Informação e Comunicação.

Evento de Segurança da Informação: ocorrência identificada de procedimento, sistema, serviço ou rede que indica possível perda de controle ou violação da política de segurança da informação, ou situação desconhecida que possa ser relevante para a segurança da informação.

Gerenciamento de Operações e Comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suportem.

Gestão de Ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada de seu controle.

Gestor de Segurança da Informação e Comunicação: é o servidor público responsável pelas ações de segurança da informação e comunicação do ANGRAPREV determinado órgão/instituição.

Identificação de Riscos: processo para localizar, listar e caracterizar elementos do risco.

Incidente de SIC: evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Política de Segurança da Informação e Comunicação: documento aprovado pela autoridade responsável do ANGRAPREV, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicação.

Proprietário de Ativos de Informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados.

Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e da comunicação.

Recursos Criptográficos: sistemas, programas, processos e equipamentos, isolados ou em rede, que utilizam algoritmo simétrico ou assimétrico, para realizar a cifração ou decifração de informações.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br

Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

Responsabilidade: dever dos agentes públicos em conhecer e respeitar todas as normas de segurança da informação e comunicação da respectiva instituição.

Risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

Segurança Física e do Ambiente: processo referente à proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização estiver presente.

Sistema Estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente.

Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao ANGRAPREV.

Transferir Risco: forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco.

Tratamento da Informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação.

Tratamento de Incidentes: processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências potenciais futuras.

Tratamento dos Riscos: processo e implementação de ações de segurança da informação e comunicação, com o objetivo de evitar, reduzir, reter ou transferir um risco.

Usuário: agente público que obteve autorização do responsável pela área interessada para acesso aos ativos de informação.

Vulnerabilidade: conjunto de fatores internos ou causas potenciais de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais devem ser evitados por ação interna de segurança da informação.

Rua Dr. Orlando Gonçalves nº 231 – Parque das Palmeiras – Angra dos Reis/RJ
Contato: (24) 3365-5260 | Site: angraprev.rj.gov.br