MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Alagoas
Pró-Reitoria de Desenvolvimento Institucional
Diretoria de Tecnologia da Informação
Comitê de Segurança da Informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Dispõe acerca da política de segurança da informação e comunicação no âmbito do Instituto Federal de Alagoas

Maceió/AL, 27 de março de 2018

Política de Segurança da Informação e Comunicação do IFAL

Ministério da Educação
Instituto Federal de Alagoas

Sérgio Teixeira Costa
Reitor

Comitê de Segurança da Informação
Handrik Palmeira Magalhães
Presidente do CSI

Diretoria de Tecnologia da Informação
Fernando Antonio Corado Carneiro
Diretor Tecnologia da Informação

LISTA DE SIGLAS E ABREVIATURAS

DICA – Disponibilidade, Integridade, Confidencialidade e Autenticidade
SI – Segurança da Informação
POSIC – Política de Segurança da Informação e Comunicação
IFAL – Instituto Federal de Alagoas
ABNT – Associação Brasileira de Normas Técnicas
IN – Instrução Normativa
GSI – Gestão de Segurança da Informação
CSI – Comitê de Segurança da Informação
ISO - International Organization for Standardization
NBR – Norma Brasileira
IEC - International Electrotechnical Comission

1. INTRODUÇÃO

1.1. Segurança da Informação (SI) é a área do conhecimento dedicada à proteção da informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação de uma instituição. A Política de Segurança da Informação e Comunicação(POSIC), por sua vez, é o documento oficial da Instituição que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a gestão da segurança da informação.

1.2. Desta forma, a política de cada órgão considera as recomendações e práticas propostas pelo Decreto n° 3.505/2000, pela IN GSI/PR n° 01/2008, pela norma internacional ABNT NBR ISO/IEC 27002:2005 e alinha-se, ainda, às demais leis e normas vigentes sobre o tema e às diretrizes estratégicas do órgão.

1.3. A política de segurança da informação é um documento estratégico, com vistas a promover o uso seguro dos ativos de informação de uma organização. Assim, deve ser entendida como uma mudança de postura e comprometimento do órgão acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem de alguma forma tenha acesso aos ativos da organização.

1.4. Esta política considera além dos aspectos técnicos, as questões comportamentais e práticas do cotidiano. Afinal, as organizações enfrentam problemas de segurança que não estão necessariamente relacionados tão somente aos aspectos tecnológicos.

1.5. Neste contexto, uma POSIC declara o comprometimento da alta direção organizacional com a finalidade de prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a Gestão da Segurança da Informação - GSI. Além disso, o estabelecimento de suas diretrizes objetiva viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade – DICA – da informação no âmbito do IFAL.

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

1.5.2. **Integridade :** Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

1.5.3. **Confidencialidade :** Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

1.5.4. **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;

2. OBJETIVOS E DESAFIOS

2.1. Instituir diretrizes e princípios de Segurança da Informação no âmbito do Instituto Federal de Alagoas – IFAL, com o propósito de mitigar a exposição ao risco a níveis aceitáveis e garantir a Disponibilidade, a Integridade, a Confidencialidade e a Autenticidade – **DICA** – das informações que suportam os objetivos estratégicos do IFAL.

2.2. Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade; são **objetivos** da Política de Segurança da Informação e Comunicação do IFAL:

2.2.1. Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional;

2.2.2. Designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação;

2.2.3. Apoiar a implantação das iniciativas relativas à Segurança da Informação;

2.2.4. Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

2.3. Ao mesmo tempo que a PSI possui objetivos, também possui desafios em sua condução e implementação. No atual contexto, com a utilização de um grande volume

de informações, desde a prestação de serviço público ao cidadão, bem como na tomada de decisões estratégicas, os objetivos propostos possuem estreito relacionamento com a segurança da informação.

2.4. Assim sendo, problemas recorrentes da falta de DICA em sistemas de informação levam à necessidade de desenvolver ações permanentes e gradativas de segurança no IFAL. Desse cenário, surgem os seguintes **desafios** a relacionados à SI:

2.4.1. Redes Sociais;

2.4.2. Computação em nuvem;

2.4.3. Aumento exponencial da utilização de dispositivos móveis;

2.4.4. Aumento da demanda de informações pelos cidadãos;

2.4.5. Leis, regulamentações e normas não unificadas;

2.4.6. Redução do custo de aquisição de tecnologias de comunicação e processamento;

2.4.7. Acesso a conexões de internet em banda larga;

2.4.8. Fragilidade na identificação de usuário ao acesso à internet;

2.4.9. Ampla disponibilidade de técnicas e ferramentas de ataque e invasão na rede e no mercado, aliado à facilidade de uso dessas ferramentas;

2.4.10. Compartilhamento de informações e ferramentas de ataque e invasão entre grupos anônimos;

2.4.11. Crescimento exponencial do crime virtual;

2.4.12. Diversificação dos perfis de ameaça: concorrente, sabotador, especulador, hacker, servidores insatisfeitos e criminosos;

2.4.13. Necessidade de tratar a informação como um recurso estratégico e econômico;

2.4.14. Crescente valorização da informação como principal ativo de gestão do Estado;

2.4.15. Crescente dependência da gestão do Estado por recursos de tecnologia da informação e comunicações;

2.4.16. Forte dependência tecnológica;

2.4.17. Interdependência entre os ativos de informação;

2.4.18. Processos de continuidade dos serviços públicos sem um grau de maturidade adequado;

2.4.19. Desconhecimento das tecnologias embutidas nas arquiteturas proprietárias; e

2.4.20. Alinhamento estratégico da SI com as atribuições institucionais dos órgãos e entidades públicos.

2.5. De uma forma geral, para tratar do tema apresentado, cabe ao Comitê de Segurança da Informação do IFAL as seguintes atribuições:

2.5.1. Promover a cultura de segurança da informação;

2.5.2. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

2.5.3. Propor à alta administração, recursos necessários às ações de segurança da informação e comunicações;

2.5.4. Coordenar o Comitê de Segurança da Informação – CSI e a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais;

2.5.5. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos da SI no órgão;

2.5.6. Responder pela SI no órgão;

2.5.7. Gerenciar a aplicação de normas e políticas de proteção aos ativos e sistemas,

de acordo com a legislação vigente;

2.5.8. Desenvolver a análise de risco e mapeamento de vulnerabilidades;

2.5.9. Elaborar o plano estratégico de Continuidade de Negócios e Recuperação de Desastres;

2.5.10. Atuar junto aos usuários finais para resolução de problemas que coloquem em risco a SI do órgão; e

2.5.11. Cuidar para que sejam observadas e aplicadas no órgão, integralmente, as normas e Políticas de Segurança da Informação e Comunicação vigentes.

3. ABRANGÊNCIA

3.1. Esta política e suas Normas Complementares aplicam-se a todos os Câmpus e polos vinculados ao Instituto Federal de Alagoas, bem como aos servidores, prestadores de serviço, colaboradores, estagiários, fornecedores consultores, externos e a quem de alguma forma tenha acesso aos ativos da organização.

3.2. Este documento, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do IFAL poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira vigente.

4. PRINCÍPIOS

4.1. O conjunto de documentos que compõe esta política deverá se guiar pelos seguintes princípios:

4.1.1. **Menor privilégio:** Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

4.1.2. **Segregação de função:** Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.

4.1.3. **Auditabilidade:** Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial.

4.1.4. **Mínima dependência de segredos:** Os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam.

4.1.5. **Controles automáticos:** Sempre que possível, controles de segurança automáticos deverão ser utilizados, especialmente os controles que dependem da vigilância humana e do comportamento humano.

4.1.6. **Resiliência:** Os sistemas e processos devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre.

4.1.7. **Defesa em profundidade:** Controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança.

4.1.8. **Exceção aprovada:** Exceções à política deverão sempre ter aprovação do Comitê de Segurança da Informação.

4.1.9. **Substituição da segurança em situações de emergência:** Controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

4.1.10. **Não-repúdio:** Serviço que fornece prova da integridade e da origem dos dados, ambos através de um relacionamento que não seja capaz de ser forjado e que possa ser verificado por quaisquer terceiros interessados, a qualquer tempo, garantindo segurança elevada de que esses dados são genuínos, e que não podem ser subsequentemente refutados. O não-repúdio é baseado na utilização pessoal e intransferível do login e senha de acesso aos sistemas do IFAL.

4.2. Esta política esta em conformidade com os princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como aos demais dispositivos legais aplicáveis.

5. DIRETRIZES GERAIS

5.1. As diretrizes de Segurança da Informação – SI – devem considerar, prioritariamente, os objetivos estratégicos, os requisitos legais a estrutura e finalidade do IFAL.

5.2. Os custos associados à Gestão da SI deverão ser compatíveis com os custos dos ativos que se deseja proteger.

5.3. A Gestão de SI deve suportar a tomada de decisões, bem como realizar a gestão de

conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos do IFAL assim como otimizar seus investimentos.

5.4. As normas e procedimento de SI do IFAL devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de SI.

5.5. **Gestão de Ativos**

5.5.1. Os ativos da organização são elementos fundamentais para a consecução dos objetivos estratégicos, portanto ações de segurança específicas deverão garantir a proteção adequada dos mesmos. Os níveis de proteção deverão variar de acordo com a criticidade do ativo para o IFAL.

5.5.2. De forma a evitar incidentes de segurança que possam danificar a imagem da instituição e interromper suas operações, os ativos de informação devem ter controles de segurança implementados independentemente do meio em que se encontram e deverão ser protegidos contra divulgação não autorizada, modificações, remoção ou destruição.

5.5.3. De forma a garantir o entendimento e a prática efetiva da SIC, as pessoas, que de alguma forma tenham acesso aos ativos de informação da organização, devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação.

5.5.4. Os processos e atividades que sustentam os serviços críticos disponibilizados pelo IFAL devem ser protegidos de forma a garantir a DICA das informações.

5.6. **Gestão de Riscos**

5.6.1. Com o objetivo de reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos da organização, deverá ser estabelecido processo que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

5.7. **Gestão de operações e comunicações**

5.7.1. Dada a importância estratégica que os recursos de processamento da informação têm para a consecução dos objetivos IFAL, ações de segurança deverão garantir a operação segura e correta desses recursos.

5.7.2. As interfaces com terceiros são importantes canais de informação que, sem um nível de segurança adequado, poderão levar a organização a uma elevada exposição a riscos. Com o objetivo de reduzir os riscos associados, o gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços.

5.7.3. A troca de informações, tanto internamente, quanto externamente, deverão ser reguladas de forma a manter o nível adequado da segurança.

5.7.4. Visando detectar o mais cedo possível atividades não autorizadas, as operações deverão ser adequadamente monitoradas.

5.8. **Controle de Acessos**

5.8.1. Com o objetivo de evitar a quebra de segurança, devem ser instituídas normas ou procedimentos que garantam o controle de acesso às informações e instalações.

5.8.2. É condição necessária para o acesso aos ativos deste IFAL, a concordância expressa e por escrito aos preceitos desta PSC.

5.8.3. Considerando que ambientes de computação móvel e de trabalho remoto são necessários para a consecução das atividades do IFAL e que podem consistir em pontos fracos do sistema de gestão de segurança, devem ser instituídas normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto.

5.9. **Gestão de Incidentes**

5.9.1. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos do IFAL.

5.10. **Gestão de Continuidade do Negócio**

5.10.1. A interrupção das atividades deste IFAL leva à suspenção de serviços críticos prestados ao cidadão e poderá resultar em grave dano à imagem da organização. Portanto, deverão ser instituídas normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços do IFAL, além de recuperar perdas de

ativos de informação a um nível estabelecido, por intermédio de ações de prevenção, resposta e recuperação.

6. POLÍTICAS TEMÁTICAS

6.1. As políticas temáticas tratam de temas específicos, tais como política de e-mail, uso da Internet, uso de telefones, segurança física, desenvolvimento de sistemas, manutenção de sistemas, segurança de redes, entre outros.

6.2. As políticas desta categoria serão definidas posteriormente em documento do Comitê de Segurança da Informação e submetidas a aprovação da Reitoria.

7. CONCEITOS E DEFINIÇÕES

7.1. **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;

7.2. **Ameaça:** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

7.3. **Ativo:** tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal;

7.4. **Ativos de Informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

7.5. **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;

7.6. **Capacitação em SI:** saber o que é segurança da informação aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na Organização como gestor de SI. [DSIC/GSIPR]

7.7. **Capacitação:** visa a aquisição de conhecimentos, capacidades, atitudes e formas de comportamento exigidos para o exercício das funções;

7.8. **Comitê de Segurança da Informação:** grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações;

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

7.10. **Conscientização em SI:** saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema.

7.11. **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;

7.12. **Controle de Acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acess;

7.13. **Custodiante:** responsável por armazenar e preservar as informações que não lhe pertencem, mas que estão sob sua custódia;

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

7.15. **Evento:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação;

7.16. **Gestão de Riscos de Segurança da Informação:** conjunto de processos que permite 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;

7.17. **Gestão de Segurança da Informação:** ações e métodos que visam à 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 à tecnologia da informação;

7.18. **Gestor de Segurança da Informação:** é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF ;

7.19. **Incidente de segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores ;

7.20. **Informação Estratégica:** toda a informação corporativa relativa à administração, planejamento, estrutura, gestão, relações internas e externas, novos produtos e tecnologias, serviços e contratos;

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

7.22. **Nível de Segurança Adequado:** será estabelecidos em documentos complementares a esta PSI;

7.23. **Política de Segurança da Informação (PSI):** documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

7.24. **Terceiro:** pessoa, não integrande do órgão ou entidade da APF, envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

7.25. **Proprietário da Informação:** pessoa ou setor que produz a informação;

7.26. **Quebra de Segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

7.27. **Riscos de Segurança da Informação e Comunicações:** potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização ;

7.28. **Segurança da Informação e Comunicações:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações ;

7.29. **Segurança de Operações e Comunicações:** responsável pela manutenção do funcionamento de serviços, sistemas e da infraestrutura que os suporta;

7.30. **Sensibilização em SI:** saber o que é segurança da informação aplicando em sua rotina pessoal e profissional;

7.31. **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;

7.32. **Vulnerabilidade:** conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

1. REFERÊNCIA NORMATIVA

1. **ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 17799:2005 (27002).** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
2. **Constituição da República Federativa do Brasil de 1988**. .
3. **Decreto no 1.171, de 22 de junho de 1994,** que dispõe sobre o Código de Ética Profissional do ervidor Público Civil do Poder Executivo Federal.
4. **Decreto no 3505, de 13 de junho de 2000**, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
5. **Decreto no 4.553, de 27 de dezembro de 2002**, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.
6. **Instrução Normativa GSI no 01, de 13 de junho de 2008**, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta e demais normas complementares.
7. **Lei 8.112, de 11 de dezembro de 1990**, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.