MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO
REITORIA

RESOLUÇÃO Nº 24 DO CONSELHO SUPERIOR, DE 10 DE AGOSTO DE 2020.

Aprova a Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - IF SERTÃO-PE.

A Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, no uso de suas atribuições legais, RESOLVE:

Art. 1º APROVAR a Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - IF SERTÃO-PE.

Art. 2º Esta resolução entra em vigor a partir da data da sua publicação.

MARIA LEOPOLDINA VERAS CAMELO:52425207368

Assinado digitalmente por MARIA LEOPOLDINA VERAS CAMELO:52425207368
DN: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=(EM BRANCO), OU=Autenticado por AR Arruda, CN=MARIA LEOPOLDINA VERAS CAMELO:52425207368
Razão: Eu sou o autor deste documento
Localização:
Data: 2020-08-10 14:52:43
Foxit Reader Versão: 9.0.1

MARIA LEOPOLDINA VERAS CAMELO
Presidente do Conselho Superior

PUBLICADO NO SITE INSTITUCIONAL EM: 10/08/2020.

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art 1º. A informação é um ativo que a Instituição tem o dever e a responsabilidade de proteger. A disponibilidade da informação de forma completa e precisa é essencial para que a mesma forneça de forma eficiente os seus serviços.

Art 2º. A elaboração e a adoção de uma Política de Segurança da Informação interna evidenciam o comprometimento da alta administração para prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação.

Art 3º. O seu propósito é estabelecer diretrizes gerais que servirão como base para as normas, procedimentos e instruções referentes à segurança da informação, atribuindo responsabilidades adequadas para o manuseio, tratamento, controle e proteção das informações pertinentes a Instituição.

Art 4º. A PSI obedece aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.

CAPÍTULO II
PRINCÍPIOS

Art 5º A Segurança da Informação do IF Sertão-PE deverá observar os seguintes princípios:

I. Ser parte integrante dos processos organizacionais;

II. Garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações;

III. Ser dinâmica e capaz de reagir a mudanças;

IV. Orientar a tomada de decisões institucionais que visem à efetividade das ações de segurança da informação e das comunicações; e

V. Estar integrada a cultura organizacional do IF Sertão-PE.

CAPÍTULO III
OBJETIVOS

Art 6º A PSI objetiva regularizar e normatizar o uso dos recursos e serviços prestados à comunidade detentores de Informação nas unidades organizacionais do IF Sertão-PE, promovendo a:

I. I. Melhoria da segurança dos usuários;

II. II. Melhoria da segurança dos meios de comunicação de dados;

III. III. Melhoria da segurança dos sistemas computacionais;

IV. IV. A cultura de segurança da informação e por meio de atividades de sensibilização, conscientização, capacitação e especialização.

CAPÍTULO IV
ESCOPO

Art. 7º A Política de Segurança da Informação do Instituto Federal do Sertão Pernambucano é uma declaração formal acerca do seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os envolvidos internamente e externamente ao IF Sertão-PE, que podem ser:

I. Servidores

II. Alunos

III. Colaboradores

IV. Estagiários

V. Prestadores de serviço que exerçam atividades no âmbito da Instituição ou;

VI. Qualquer cidadão que tenha acesso a dados ou informações no âmbito do Instituto.

Art 8º Esta Política também é extensiva ao relacionamento do IF Sertão-PE com outros órgãos e instituições públicas ou privadas.

CAPÍTULO V
CONCEITOS E DEFINIÇÕES

I. **Ameaça**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
II. **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar seu risco;
III. **Ativo**: qualquer coisa que tenha valor para a organização;
IV. **Autenticidade**: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
V. **Avaliação de riscos:** processo por intermédio do qual se compara o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;

VI. **Colaborador:** pesquisador que colabora com atividades de ensino, pesquisa, orientação e extensão, normalmente, de um Programa de Pós-Graduação por um período pré-determinado de tempo, em regime integral. Possui vínculo funcional-administrativo com outras instituições, brasileiras ou internacionais, e são liberados temporariamente de suas atividades na instituição de origem por meio de um acordo formal;

VII. **Comitê Gestor de Segurança da Informação:** grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do IF SERTÃO-PE;

VIII. **Comunicação Oficial:** tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IF SERTÃO-PE, de atividades especiais ou ainda de projetos específicos;

IX. IX. **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

X. **Contingência**: indisponibilidade ou perda de integridade da informação que os controles de segurança não tenham conseguido evitar;

XI. **Controle:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XII. **Custodiante do Ativo de Informação:** 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;

XIII. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda da Administração;

XIV. **Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR):** grupo com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

XV. **Gestor de Segurança da Informação (GSI):** é responsável pelas ações de segurança da informação e das comunicações no âmbito do IF Sertão-PE, designado formalmente pelo Reitor;

XVI. **Incidente de Segurança da Informação:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XVII. **Identificação de riscos:** processo de localização, enumeração e caracterização dos elementos do risco;

XVIII. **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

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

XX. **Plano de Continuidade de Negócios:** documentação dos procedimentos e informações necessárias para que a organização mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

XXI. **Plano de Gerenciamento de Incidentes:** plano de ação claramente definido e documentado, para ser utilizado quando ocorrer um incidente e que especifique as pessoas, recursos, serviços e outras ações que forem necessárias para implementar o processo de gerenciamento de incidentes;

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

XXIII. **Quebra de Segurança:** ação ou omissão, intencional ou acidental, que resulte no comprometimento da Segurança da Informação e Comunicações;

XXIV. **Recursos de Processamento da Informação:** qualquer sistema, serviço ou infraestrutura de processamento da informação, ou as instalações físicas que os abriguem;

XXV. **Termo de Responsabilidade:** acordo de confidencialidade e não divulgação de informações, que atribui responsabilidades ao servidor e ao administrador de serviço quanto ao sigilo e à correta utilização dos ativos de propriedade da Instituição ou por ela custodiados;

XXVI. **Tratamento da Informação:** recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive das sigilosas;

XXVII. **TI:** Tecnologia da Informação;

XXVIII. **Usuário**: pessoa física seja servidor ou equiparado, empregado ou prestador de serviços, aluno e pessoa da sociedade civil habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura de Termo de Responsabilidade;

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

CAPÍTULO VI
DIRETRIZES GERAIS

Art 9º A segurança da informação tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos.

Art 10º Todo usuário é responsável e deve estar comprometido com a segurança da informação do IF Sertão-PE.

Art 11º Somente atividades lícitas e éticas consoantes às normativas do IF Sertão-PE deverão ser realizadas pelos usuários durante o uso dos ativos de informação institucionais.

Art 12º O acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida,

utilizada ou armazenada pelo IF Sertão-PE é considerada seu patrimônio e deve ser protegida;

Art 13º Para cada uma das diretrizes Gerais serão integradas Normas Complementares específicas, os quais destinam à proteção da informação e à disciplina de sua utilização.

Tratamento da Informação

I. Os critérios gerais aplicáveis à classificação e ao tratamento da informação serão definidos por normas complementares, elaborados pelo Comitê Gestor de Segurança da Informação (CGSI), com a participação de representantes das unidades do IF Sertão-PE que produzem, recepcionam ou custodiam informações essenciais às atividades finalísticas.

II. Toda informação documentada produzida ou recebida no âmbito do IF Sertão-PE pertence à própria Instituição, possui valor e deve ser protegida para permitir o uso adequado à consecução dos objetivos institucionais.

III. As informações deverão ser classificadas e protegidas de acordo com o grau de sigilo e sensibilidade, respeitando o ciclo vital dos documentos exigido pelas atividades do IF Sertão-PE.

IV. A gestão da informação abrange os documentos produzidos, recebidos e armazenados, independentemente da forma ou do suporte, estejam eles em ambientes convencionais, digitais, não digitais ou híbridos.

Segurança Física e do Ambiente

I. Os equipamentos e as instalações de processamento de informação críticas ou sensíveis deverão ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

II. Deverão ser utilizadas barreiras de segurança para a proteção de áreas que contenham informações e instalações de processamento da informação.

Gestão de Incidentes em Segurança da Informação

I. A gestão de incidentes em segurança da informação tem por objetivo assegurar que fragilidades e incidentes em segurança da informação sejam identificados, para permitir a tomada de ação corretiva em tempo hábil.

II. As diretrizes específicas e procedimentos próprios relacionados ao tratamento de incidentes em redes computacionais deverão ser fixados em norma complementar.

III. Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas.

IV. O tratamento do incidente deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, de acordo com as normas já existentes no ordenamento jurídico vigente.

Gestão de Ativos da Informação

I. Os ativos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos.

II. Deverão ser instituídas normas complementares que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações, equipamentos e sistemas de informação, observadas por todos os usuários.

Gestão do Uso dos Recursos Operacionais e de Comunicações

I. Os sistemas institucionais, os serviços corporativos de correio eletrônico, mensagens instantâneas, Intranet e Internet devem ter seu uso orientado para o interesse do IF Sertão-PE.

II. Os recursos disponibilizados pelo IF Sertão-PE, e de sua propriedade, são fornecidos com o propósito de garantir o desempenho das suas atividades.

III. O serviço de correio eletrônico disponibilizado pelo IF Sertão-PE constitui recurso do Instituto disponibilizado na rede de comunicação de dados para aumentar a agilidade, segurança e economia da comunicação oficial e formal.

IV. A Gestão do Uso dos Recursos Computacionais Operacionais e de Comunicações disponibilizados pelo IF Sertão-PE será definida por norma complementar específica.

Controles de Acesso

I. O acesso aos ambientes físicos e computacionais das Unidades Organizacionais do IF Sertão-PE deverá ser controlado e concedido somente a pessoas identificadas e autorizadas.

II. A autorização, o acesso e o uso da informação e dos recursos de tecnologia da informação e comunicações devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário, e qualquer outra forma de uso ou acesso além do necessário dependem de autorização do proprietário do ativo de informação, em acordo às normas já existentes no ordenamento jurídico vigente.

III. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do IF Sertão-PE.

IV. Todos os sistemas de informação do Instituto, automatizados ou não, deverão ter um custodiante do ativo da informação, formalmente designado pelo proprietário do ativo de informação, que deve definir os privilégios de acesso às informações, em acordo às normas já existentes no ordenamento jurídico vigente.

Gestão de Riscos

I. Deverá ser estabelecido o processo de Gestão de Riscos dos ativos de informação e de processamento do IF Sertão-PE, visando à identificação,

avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação.

II. O escopo, as diretrizes e a metodologia do processo de Gestão de Riscos dos ativos de informação e de processamento do IF Sertão-PE serão definidos em norma complementar.

Gestão de Continuidade

I. Deverá ser estabelecido o Programa de Gestão da Continuidade de Negócios a fim de minimizar os impactos decorrentes de incidentes de Segurança da Informação sobre as atividades institucionais, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

II. O Programa de Gestão da Continuidade de Negócios será elaborado por grupo de trabalho formalmente instituído pelo Comitê Gestor de Segurança da Informação.

Auditoria e Conformidade

I. A avaliação da conformidade em Segurança da Informação deverá considerar a PSI, suas normas complementares e os requisitos legais pertinentes.

II. O uso dos recursos de TI disponibilizados pelo IF Sertão-PE é passível de monitoramento e auditoria e deverão ser implementados e mantidos, mecanismos que permitam a sua rastreabilidade.

CAPÍTULO VII

ESTRUTURA PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art 14º A Gestão de Segurança da Informação (GSI) deverá apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação.

Art 15º A GSI deverá compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança da informação, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do IF Sertão-PE.

Art 16º De forma a estruturar a gestão da segurança da informação, o IF Sertão-PE, deverá designar ou instituir, ao menos:

I - O Gestor de Segurança da Informação;

II - O Comitê Gestor de Segurança da Informação ou estrutura equivalente; e

III - Uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) ou estrutura equivalente.

CAPÍTULO VIII
(COMPETÊNCIAS E RESPONSABILIDADES)

Art.17º Como forma de garantir o sucesso da gestão da segurança da informação no IF Sertão-PE, é necessário a definição dos papéis de todos os envolvidos, bem como suas respectivas responsabilidades conforme descrito:

I - Conselho Superior (CONSUP) - Será responsável pela aprovação da Política de Segurança da Informação.

II - Reitor (a) - responsável pelo Instituto Federal, que compete:

a. Designar um Gestor de Segurança da Informação do IF Sertão-PE;

b. Designar os membros do Comitê de Segurança da Informação ou estrutura equivalente.

c. Designar a Equipe de Tratamento Incidentes de Segurança da Informação.

d. Viabilizar o desenvolvimento dos trabalhos do Comitê Gestor de Segurança da Informação e da Equipe de Tratamento Incidentes de Segurança da Informação.

e. Assegurar os recursos necessários para a implementação e gestão da PSI do IF Sertão-PE.

III - **O Comitê Gestor de Segurança da Informação possui as seguintes atribuições:**

a. assessorar a implementação das ações de segurança da informação;

b. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

c. participar da elaboração da Política de Segurança da Informação e das normas complementares de segurança da informação;

d. propor alterações à Política de Segurança da Informação e às normas complementares de segurança da informação; e

e. deliberar sobre normas complementares de segurança da informação.

f. Será responsável pela aprovação das Normas Complementares propostas pelos membros do CGSI, podendo submetê-las ao CONSUP quando necessário.

IV - **Compete ao gestor de segurança da informação:**

a. coordenar o Comitê de Segurança da Informação;

b. coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

c. assessorar a alta administração na implementação da Política de Segurança da Informação;

d. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

e. promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

f. incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

g. Propor programa orçamentário específico junto com o Comitê Gestor para capacitação da equipe de segurança e para as ações de segurança da informação e comunicação;

h. acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

i. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

j. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

k. manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

V - Compete Equipe de Tratamento e Resposta a Incidente Cibernético (ETIR)

a. Tratar quaisquer incidentes de segurança em redes de computadores ocorridas no IF Sertão-PE

b. Promover a cultura de Segurança da Informação;

c. Executar o Plano de Continuidade da instituição no caso de situação de falhas e desastres.

VI - Competem aos usuários:

a. Cumprir as políticas, as normas, os procedimentos e as orientações de segurança da informação;

b. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados;

c. Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades acadêmicas e institucionais.

Art.18º Deverá ser elaborado regimento interno para dispor sobre a organização e o funcionamento do Comitê Gestor de Segurança da Informação.

Art.19º Deverá ser elaborado documento de constituição da Equipe de Tratamento e Resposta a Incidentes Cibernéticos, o qual designará suas atribuições e seu escopo de atuação.

Art.20º Deverá ser elaborado normativa complementar para dispor sobre o funcionamento da Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

CAPÍTULO IX
REFERÊNCIAS LEGAIS E NORMATIVAS

I - Decreto 1.171, de 24 de junho de 1994 que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

II - Lei no 9.983, de 14 de julho de 2000: Altera o Decreto Lei no 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

III - ABNT ISO/IEC GUIA 73: 2005 - Gestão de Riscos / Vocabulário – Recomendações para uso em normas;

IV - Lei nº. 12.527, de 18 de novembro de 2011, que regula o acesso à informação (Lei de Acesso à Informação).

V - Decreto no 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;

VI - ABNT NBR ISO/IEC 27001:2013 - Código de prática para controles de segurança da informação;

VII - ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;

VIII - o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - a Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

X - o Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

XI – Instrução Normativa nº 1, de 27 de maio de 2020, dispõe sobre a sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

CAPÍTULO X
PENALIDADES

Art.21º Nos casos em que houver o descumprimento ou violação de um ou mais itens da PSI e de suas normas complementares, poderão acarretar em suspensão de privilégios de acesso aos recursos computacionais e implicar em penalidades previstas em lei nos âmbitos administrativo, civil, penal e ético;

Art.22º Nos casos de suspensão de privilégios de acesso aos recursos computacionais, o período de suspensão é de, no máximo, 90 (noventa) dias, contado a partir da comprovação do descumprimento ou violação do usuário, verificada pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do IF Sertão – PE.

Art.23º Caberá ao Comitê Gestor de Segurança da Informação esclarecer os casos omissos a esta Política.

CAPÍTULO XI
REVISÃO E ATUALIZAÇÃO

Art.24º Esta Política bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 04 (quatro) anos.

CAPÍTULO XII
PUBLICAÇÃO

Art.25º A Política e as Normas Complementares de Segurança da Informação e suas atualizações deverá ser divulgadas pelos canais de comunicação do IF Sertão-PE a todos os servidores, usuários, prestadores de serviço, contratados e colaboradores que habitualmente integram o quadro funcional do IF Sertão-PE dispostas de maneira que seu conteúdo poderá ser consultado a qualquer momento.

Art.26º Após aprovação de novas normativas ou atualizações dos documentos da PSI, deverão ser divulgados novos comunicados aos interessados pela área responsável por sua proposição e manutenção.

CAPÍTULO XIII
DAS DISPOSIÇÕES FINAIS

Art.27º Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação devem ser direcionados ao Comitê Gestor de Segurança da Informação.

Art. 28º A presente política entra em vigor a partir da data de sua publicação.