POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES - POSIC

Dispõe sobre a Política de Segurança da Informação e Comunicação do Instituto Federal de Brasília.

INTRODUÇÃO

Este documento institui a Política de Segurança da Informação e das Comunicações e se aplica a todas as unidades regimentais do Instituto Federal de Brasília, a qual deverá ser adotada e cumprida por todos os servidores, colaboradores, consultores externos, estagiários, alunos e prestadores de serviço que exerçam atividades, ou quem tenha acesso a dados ou informações no ambiente do IFB.

CAPÍTULO I
DO ESCOPO

Art. 1 – A Política de Segurança da Informação e das Comunicações - POSIC do Instituto Federal de Educação, Ciência e Tecnologia de Brasília – IFB, tem por objetivo estabelecer diretrizes, normas, procedimentos e responsabilidades visando a continuidade dos processos institucionais críticos e à manutenção do bom uso da informação em todos os seus aspectos.

Art. 2 – A POSIC deve atender aos preceitos constitucionais, ao arcabouço legal vigente, aos documentos normativos e administrativos que regem a Administração Pública Federal, bem como estar em conformidade com requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.
Parágrafo único: Os fundamentos legais e normativos que fundamentam esta POSIC estão elencados no Capítulo III deste documento.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3 – Para fins desta Portaria Normativa, entende-se por:
I – **Agente público:** aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao IFB;
II – **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição [ISO/IEC 13335-1:2004];

III - **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco;
IV - **Ativo de Informação**: dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados no IFB;
V - **Ativo de Tecnologia da Informação**: composto por ativos de software e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações;
VI - **Auditoria em Segurança da Informação:** processo de avaliação da situação atual dos controles de segurança da informação implementados;
VII - **Contingência:** indisponibilidade ou perda de integridade da informação que os controles de segurança não tenham conseguido evitar;
VIII - **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. Controle também é usado como sinônimo para proteção ou contramedida;
IX - **Custodiante do ativo**: unidade administrativa responsável pelo armazenamento, operação, administração e preservação de ativos;
X - **Custodiante da informação**: colaborador responsável pela guarda adequada do dado;
XI - **Dado:** representação de uma determinada situação ou evento em determinado espaço e tempo, sob uma forma apropriada ao armazenamento, processamento ou transmissão, não fornecendo julgamento nem interpretação para a tomada de decisões;
XII - **Dispositivo ou recurso de tecnologia da informação e comunicações (TIC):** todo e qualquer equipamento que permita a armazenagem e/ou veiculação de informações ou dados, por qualquer processo, seja ele óptico, gráfico, magnético, eletrônico ou outros;
XIII - **Documento:** toda a base de conhecimento, fixada materialmente, suscetível de ser utilizada para consulta, estudo ou prova;
XIV – **Evento de segurança da informação:** 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 [ISO/IEC TR 18044:2004];
XV – **Gestor:** agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas do uso da informação;
XVI – **Incidente:** é indicado por um simples ou por uma série de eventos de Segurança da Informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação;
XVII – **Informação:** dados e fatos dotados de relevância e propósito que foram organizados e comunicados de forma coerente e com significado e a partir dos quais se podem tirar conclusões e interpretações;
XVIII - **Plano de continuidade de negócios:** conjunto de procedimentos que devem ser adotados quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços;
XIX – **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e das Comunicações;
XX - **Risco:** combinação da probabilidade de ocorrência de um evento e de suas consequências;
XXI - **Segurança da informação:** preservação da confidencialidade, da integridade e da disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também estão envolvidas;

XXII - **SIC:** Segurança da Informação e Comunicações;
XXIII - **Tratamento da informação:** recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
XXIV - **Usuário externo:** qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao IFB;
XXV - **Usuário interno:** qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente ao IFB;
XXVI – **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4 – As referências legais e normativas utilizadas para a elaboração da POSIC são:
I – Constituição Federal de 1988, reformada em 2008;
II – Lei nº 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;
III – Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;
IV – Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (Revogado pelo Dec. 9.637 de 2018);
V – 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, e dá outras providências;
VI – Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores – Internet;
VII – Lei nº 9.610, de 19 de fevereiro de 1998, altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências;
VIII – Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
IX – Norma Complementar no 03/IN01/DSIC/GSI/PR, de 03 de julho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta;
X – Norma ABNT NBR ISO/IEC 27001:2006 – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;
XI – Norma ABNT NBR ISO/IEC 27002:2013 – Técnicas de segurança - Código de práticas para a segurança da informação;

XII - Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 de outubro de 2008, que estabelece a Metodologia de Gestão de Segurança da Informação e Comunicações;
XIII - Norma Complementar nº 04/IN01/DSIC/GSIPR, de 25 de fevereiro de 2013, que estabelece Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;
XIV - Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;
XV - Norma Complementar nº 06/IN01/DSIC/GSIPR, de 23 de novembro de 2009, que estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
XVI - Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;
XVII - Norma Complementar nº 10/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
XVIII - Norma Complementar nº 11/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, que estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;
XIX – Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
XX – Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
XXI – Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12965 de 2014;
XXII – Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, dispõe sobre a governança da segurança da informação, altera o Decreto nº 2.295 de 1997 e revoga os decretos nº 3.505 de 2000 e nº 8.135 de 2013;
XXIII - Portaria Normativa nº 003, de 30 de março de 2012, que normatiza o uso do correio eletrônico institucional em atendimento à Resolução nº 34/2011 - CS/IFB.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 5 – Esta política abrange onze aspectos básicos da Segurança da Informação e Comunicação, destacados a seguir:

I – **Autenticidade:** princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;
II - **Ciência:** todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;
III **- Confidencialidade:** somente pessoas devidamente autorizadas pelo gestor da informação devem ter acesso à informação não pública;
IV - **Criticidade:** princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;
V - **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;
VI - **Ética:** todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFB devem ser respeitados;
VII – **Integridade:** somente operações de alteração, supressão e adição autorizadas pelo IFB devem ser realizadas nas informações;
VIII – **Legalidade:** além de observar os interesses do IFB, as ações de Segurança da Informação e Comunicações levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e direitos de uso;
IX – **não-Repúdio:** é a capacidade de garantir que um usuário ou sistema realmente realizou uma operação em um sistema da informação, não permitindo a existência de dúvidas ou questionamentos sobre a sua realização;
X – **Proporcionalidade:** o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no IFB serão adequados ao entendimento administrativo e ao valor do ativo a proteger;
XI – **Responsabilidade:** as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os servidores do IFB são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação e Comunicações advindas desta política.

CAPÍTULO V
DAS DIRETRIZES

Seção I
Das Disposições Gerais

Art. 6 – O cumprimento desta política de segurança e os documentos delas advindos deverão ser avaliados periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê Gestor de Segurança da Informação e das Comunicações (CGSIC-IFB), ou pelo CGD caso aquele ainda não estiver instituído, buscando a

certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 7 – O CGSIC-IFB deve auxiliar o Comitê de Governança Digital na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias do IFB e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 8 – O CGSIC deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 9 – O IFB, além das diretrizes estabelecidas nesta POSIC, deve também se orientar pelas melhores práticas e procedimentos de SIC, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 10 – É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas ou custodiadas pelo IFB.

Art. 11 – Os contratos firmados pelo IFB devem conter cláusulas que determinem a observância da POSIC e seus respectivos documentos.

Art. 12 – Serão elaboradas normas complementares para esse documento.

Seção II
Da Abrangência

Art. 13 – As diretrizes, normas, procedimentos, manuais e quaisquer outros documentos advindos desta POSIC aplicam-se aos servidores, corpo discente, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, executar atividades vinculadas ao IFB.
Parágrafo único: Todos são responsáveis e devem estar comprometidos com a segurança da informação e das comunicações.

Art. 14 – Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo IFB devem atender a esta norma.

Art. 15 – Esta política também se aplica, no que couber, ao relacionamento do IFB com outros órgãos e entidades públicas ou privadas.

Seção III
Das Instâncias

Art. 16 – O Comitê de Governança Digital (CGD), antigo Comitê Gestor de Tecnologia da Informação (CGTI), instituído pela Portaria IFB nº 2 de maio de 2016, é uma instância de natureza consultiva, propositiva, de caráter permanente, vinculado à Reitoria, que determina as prioridades dos programas de investimentos em Tecnologia da Informação (TIC), as estratégias de TIC e aprova as Políticas de segurança da informação e comunicações do Instituto;

Art. 17 – São instâncias de implementação, fiscalização e atualização desta POSIC:
I – O Comitê de Governança Digital (CGD);
II – Comitê Gestor da Segurança da Informação e das Comunicações (CGSIC) do IFB é um órgão de assessoramento da Reitoria a ser instituído no IFB e composto por uma equipe multidisciplinar, com natureza consultiva nas questões concernentes às suas atribuições definidas em processo específico;
III – Diretoria de Tecnologia da Informação e Comunicação (DTIC): instância administrativa/ executiva responsável por propor as políticas e programas do IFB na área de informática e telecomunicações, bem como por sua implementação e gestão;
IV – Equipe de Tratamento de Incidentes de Redes de Computadores (ETIR): instância a ser instituída, responsável a dar tratamento de primeiro nível aos incidentes de segurança da informação e das comunicações;
V – Unidade Administrativa: qualquer instância administrativa do IFB a exemplo dos Campi, unidades ligadas aos Campi, núcleos de pesquisa e centros com funcionalidades específicas.

Seção IV
Do Tratamento da Informação

Art. 18 – Todo ativo de informação criado, adquirido ou custodiado pelo agente público, no exercício de suas atividades, é considerado um bem e deve ser protegida de acordo com as regulamentações de segurança existentes com o objetivo de minimizar riscos às atividades e serviços prestados pelo IFB, preservando sua imagem.

Art. 19 – As informações produzidas ou custodiadas pelo IFB devem ser descartadas conforme o seu nível de classificação.

Seção V
Da Classificação da Informação

Art. 20 – As informações custodiadas ou de propriedade do IFB devem ser classificadas levando-se em consideração seu valor, criticidade, sensibilidade e requisitos legais e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.

Art. 21 – O proprietário da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade de acordo com o plano de classificação da instituição ou se não houver, seguir o que estabelece o Conarq.

Art. 22 – A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Seção VI
Da Sensibilização, Conscientização e Capacitação

Art. 23 – O IFB desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Seção VII
Da Gestão dos Ativos de Informação

Art. 24 – O custodiante do ativo de informação deve ser o responsável pelo armazenamento, operação, administração e preservação do ativo de informação.

Art. 25 – Os bens ativos de informação devem:
I – Ser inventariados e protegidos;
II – Ser identificados os seus proprietários e custodiantes;
III – Ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
IV – Ter a sua entrada e saída nas dependências do IFB autorizadas e registradas por autoridade competente;
V – Ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;
VI – Ser regulamentados por norma específica quanto a sua utilização; e
VII – Ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares.

Art. 26 – O proprietário do ativo de informação deve criar e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 27 – Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 28 – Os sistemas de informação e os aplicativos do IFB devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 29 – O acesso dos usuários externos aos ativos de informação (bem patrimonial) e sua utilização, quando autorizados, deve ser condicionado à ciência e ao aceite do responsável, conforme dita esta POSIC.

Seção VIII
Da Aquisição, Do Desenvolvimento e Da Manutenção de Sistemas

Art. 30 – A Equipe em SIC deve estabelecer, em norma específica, critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Art. 31 – O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Seção IX
Do Plano de Investimento em SIC

Art. 32 – Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos.

Art. 33 – O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco e que será submetido ao Comitê de Governança Digital do IFB (CGD-IFB).

Seção X
Da Propriedade Intelectual

Art. 34 – Na condição de propriedade intelectual, protegida por lei, nenhum aplicativo poderá ser utilizado no IFB sem a devida aquisição da licença de uso.
Parágrafo único: A gestão das licenças de uso dos aplicativos será de responsabilidade do gestor de cada unidade administrativa.

Seção XI
Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 35 – Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIC.

Art. 36 – O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta POSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no IFB.

Art. 37 – Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 38 – Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

Seção XII
Da Gestão de Mudanças

Art. 39 – Deve ser definido um processo adequado e objetivo de gestão de mudanças que será detalhado em norma específica.

Seção XIII
Da Gestão de Descarte

Art. 40 – Nenhuma mídia armazenadora de dados deve ser descartada sem o devido tratamento, objetivando a segurança das informações nela contidas.
Parágrafo único: Entende-se por mídia qualquer dispositivo físico capaz de armazenar dados, a exemplo de mídias magnéticas, ópticas, eletrônicas e papel.

Art. 41 – Caberá à Política de Descarte a ser estabelecida no IFB definir, em função da criticidade da informação, o tempo para destruição física da mídia e para o seu armazenamento e reaproveitamento.

Seção XIV
Do Tratamento de Incidentes de Rede

Art. 42 – O CGSIC-IFB deverá constituir a ETIR.
§ 1º Na constituição da ETIR, o IFB deverá definir o modelo de implantação que melhor se adequar às necessidades e limitações da instituição, dentre os especificados na Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009, e observar as diretrizes nela estabelecidas e nas demais normas relacionadas ao tema.
§ 2º Independente do modelo estabelecido, deverá ser designado formalmente o Agente Responsável, que terá, dentre outras atribuições, a de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.
§ 3º O Agente escolhido será o responsável por criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe ou Equipes que compõem a ETIR.
§ 4º A ETIR deverá possuir um regimento interno próprio e que deverá ser referendado pelo CGSIC-IFB.

Art. 43 – A Equipe de SIC deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo do CTIR gov.

Seção XV
Da Gestão de Riscos

Art. 44 – A Equipe de Segurança da Informação e Comunicação deve estabelecer processos de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.

Art. 45 – A GRSIC é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e das Comunicações, levando em consideração o planejamento, a execução, análise crítica e melhoria da SIC no IFB.

Art. 46 – As proteções devem estar alinhadas aos riscos identificados.

Seção XVI
Da Gestão de Continuidade

Art. 47 – O IFB deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

Art. 48 – As ações de continuidade do IFB devem ser adotadas por todos os titulares de unidade administrativa, de forma a proteger a reputação e a imagem institucional.

Art. 49 – As informações de propriedade ou custodiadas pelo IFB, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades do órgão. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservam sua integridade, conforme o nível de classificação atribuído.

Seção XVII
Da Auditoria e Conformidade

Art. 50 – Deve ser realizada, com periodicidade mínima anual, a verificação de conformidade das práticas de SIC do IFB desta POSIC e de suas normas e procedimentos complementares, bem como com a legislação específica de SIC.

Art. 51 – A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados pelo IFB.

Art. 52 – A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pelo CGSIC ou, caso ainda não tenha sido estabelecido, pelo CGD.

Art. 53 – O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos percebidos.

Art. 54 – Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SIC por período superior a 2 (dois) anos.

Art. 55 – A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 56 – Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

Seção XVIII
Dos Controles de Acesso

Art. 57 – O IFB deve sistematizar a concessão de acesso como forma de evitar a quebra de segurança da informação e comunicações.

Art. 58 – O acesso às informações custodiadas ou de propriedade do IFB pelos agentes públicos deve ser restrito ao necessário para desempenho de suas funções.

Art. 59 – O acesso físico às instalações do IFB deverá ser regulamentado com o objetivo de garantir a segurança dos agentes públicos e a proteção dos seus ativos.

Seção XIX
Do Uso de Recursos Computacionais e Comunicações

Art. 60 – O uso de recursos computacionais e de comunicações do IFB pelos agentes públicos deve ser direcionado exclusivamente para realização das atividades profissionais desempenhadas para o órgão no limite dos princípios da ética, razoabilidade e legalidade.

Art. 61 – Não é permitida a utilização de programas que violem direitos autorais, conforme legislação em vigor.

Seção XX

Das Normas Específicas de Segurança

Art. 62 – Os aspectos de segurança física e do ambiente (controles de acesso), lógica (uso de e-mail, internet) e de recursos humanos (engenharia social), serão tratados em documentos independentes, a fim de complementar com maior especificidade e detalhamento as normas e recomendações de segurança no trato das informações.
Parágrafo único: Todos os procedimentos relacionados à Segurança da Informação, definidos em instruções específicas, devem estar de acordo com esta Política, e uma vez divulgados, passam a ser parte integrante desta.

CAPÍTULO VI
DAS PENALIDADES

Art. 63 – Nos casos em que houver o descumprimento ou violação de um ou mais itens da POSIC ou de suas Normas, procedimentos ou atividades pertinentes à Segurança da Informação e Comunicação, estes serão tratados conforme legislação e regulamentos internos aplicáveis.

CAPÍTULO VII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 64 – É dever do agente público do IFB conhecer e zelar pelo cumprimento da POSIC.

Art. 65 – Os agentes públicos são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como crachá, *login*, senha eletrônica, certificado digital e endereço de correio eletrônico.
Parágrafo único: A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

Art. 66 – Cabe a Alta Gestão do IFB:
I – Comprometer-se em proteger todos os ativos de informação da instituição;
II – Formalizar esta POSIC;
III – Garantir a provisão dos recursos necessários para a implementação da POSIC no IFB;
IV – Promover no IFB a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização.

Art. 67 – Cabe ao CGD
I – Aprovar a Política de Segurança da Informação;
II – Instituir o Comitê Gestor de Segurança da Informação – CGSI;
III – Aprovar as normas específicas de Segurança da Informação;
IV – Desempenhar as atividades do CGSI enquanto este não for instituído;

V – Exercer outras atribuições que lhes forem atribuídas em regimento interno.

Art. 68 – Cabe ao CGSI:
I – Desenvolver a cultura de segurança da informação e das comunicações na Instituição;
II – Coordenar as ações de segurança da informação e das comunicações;
III – Propor, aprovar e publicar normas e procedimentos complementares à POSIC;
IV – Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC;
V – Avaliar criticamente a POSIC, visando a sua aderência aos objetivos institucionais do IFB e à legislação vigente, e propor sua revisão, quando necessário;
VI – Indicar o Gestor de Segurança da Informação e das Comunicações;
VII – Instituir e implementar a Equipe de Tratamento de Incidentes de Redes de Computadores (ETIR), supervisionar suas ações e referendar o seu Regimento Interno;
VIII – Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e das comunicações;
IX – Constituir grupo de trabalho para realizar auditoria de segurança da informação e das comunicações;
X – Receber e consolidar os resultados dos trabalhos de auditoria de segurança da informação e das comunicações e remetê-los à Reitoria;
XI – Responder às demandas dos órgãos de controle quando referentes à segurança da informação e das comunicações no IFB;
XII – Realizar e/ou acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e das comunicações;
XIII – Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e das comunicações;
XIV – Propor o Plano de Investimentos em Segurança da Informação e das Comunicações do IFB;
XV – Desenvolver o Plano de Continuidade de Negócios para o IFB, dentro de sua área de competência;
XIV – Assessorar a Reitoria nos assuntos relativos à segurança da informação e das comunicações;
XV – Desempenhar as atividades do ETIR enquanto este não estiver instituído.

Art. 69 – Cabe à ETIR:
I – Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;
II – Promover a recuperação de sistemas;
III – Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;
IV – Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
V – Analisar ataques e intrusões na rede do IFB;
VI – Executar as ações necessárias para tratar quebras de segurança;
VII – Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
VIII – Cooperar com outras equipes de Tratamento e Resposta a Incidentes;

IX – Participar em fóruns, redes nacionais e internacionais relativas à SIC;
X – Aprovar o seu regimento interno.

Art. 70 – Cabe ao Gestor do Ativo de Informação:
I – Promover a segurança dos ativos de informação sob sua responsabilidade;
II – Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta POSIC;
III – Conceder e revogar acessos aos ativos de informação;
IV – Comunicar à ETIR a ocorrência de incidentes de SIC;
V – Designar custodiante dos ativos de informação, quando aplicável.

Art. 71 – Cabe ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso de execução/alteração, de acordo com os requisitos definidos pelo gestor da informação e em conformidade com esta POSIC.
Parágrafo único: O acesso de leitura às informações obedecerá ao disposto na Lei de Acesso à Informação Pública (Lei nº 12.527/2012).

Art. 72 – Cabe ao titular da unidade administrativa:
I – Corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua subordinação;
II – Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;
III – Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;
IV – Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;
V – Realizar o tratamento e a classificação da informação;
VI – Autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;
VII – Comunicar à ETIR os casos de quebra de segurança; e
VIII – Manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 73 – Cabem aos terceiros e fornecedores, conforme previsto em contrato:
I – Tomar conhecimento desta POSIC;
II – Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;
III – Fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 74 – Cabem aos usuários:
I – Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta POSIC, bem como os demais normativos e resoluções relacionados à SIC;
II – Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação;
III – Comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações ao ETIR ou ao responsável máximo pela unidade administrativa.

CAPÍTULO VIII
DA ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 75 – Fica instituído, no âmbito do IFB o Comitê Gestor de Segurança da Informação e Comunicações, com as seguintes competências:
I – Assessorar na implementação das ações de segurança da informação e comunicações no Instituto;
II – Constituir grupos de trabalho para tratar temas e propor soluções específicas sobre segurança da Informação e comunicações; e
III – Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com a legislação existente sobre o tema.
Parágrafo único: O Comitê Gestor de Segurança da Informação e Comunicações será constituído por meio de portaria do reitor.

Art. 76 – Fica instituído, no âmbito do IFB o Gestor de Segurança da Informação e Comunicações, com as seguintes competências:
I – Promover cultura de segurança da informação e comunicações;
II – Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III – Propor recursos necessários às ações de segurança da informação e comunicações;
IV – Coordenar a equipe de tratamento e resposta a incidentes em redes computacionais;
V – Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
VI – Manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações; e
VII – Propor normas relativas à segurança da informação e comunicações.
Parágrafo único: O gestor de segurança da informação e comunicações será designado em expediente próprio e deverá reportar-se sempre ao Comitê Gestor de Segurança da Informação e Comunicações.

Art. 77 – Fica instituída, no âmbito do IFB, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), conforme a Norma Complementar Nº 5, de 14 de agosto de 2009.
Parágrafo único: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) será constituída por meio de portaria do reitor.

CAPÍTULO IX
DA ATUALIZAÇÃO

Art. 78 – A POSIC e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 2 (dois) anos.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 79 – O descumprimento ou violação de um ou mais itens desta Política de Segurança da Informação e Comunicações poderá resultar na aplicação de sanções administrativas, penais ou civis.

Art. 80 – Os casos omissos serão resolvidos pelo Comitê de Governança Digital (CGD).

CAPÍTULO XI
DA DIVULGAÇÃO

Art. 81 – A POSIC e suas atualizações, bem como as normas complementares, devem ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados que habitualmente trabalham no IFB.

CAPÍTULO XII
DA VIGÊNCIA

Art. 82 – Esta Portaria Normativa entra em vigor na data de sua assinatura.