SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO

RESOLUÇÃO Nº. 13 DO CONSELHO SUPERIOR,

DE 22 DE JUNHO DE 2016.

A Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, no uso de suas atribuições legais e após deliberação dos membros do Conselho Superior ocorrida na 3ª Reunião Ordinária do exercício de 2016, resolve:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicação (POSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano.

Art. 2º Aprovar o Regimento Interno do Comitê Gestor de Segurança da Informação – CGSI – do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano.

Art. 3º Esta Resolução entra em vigor a partir da data da sua publicação.

Maria Leopoldina Veras Camelo
Presidente do Conselho Superior
IF Sertão PE

PUBLICADO NO SITE INSTITUCIONAL EM: **12/08/2016**

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

DO SERTÃO PERNAMBUCANO

POLITICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC)

Petrolina/PE

2016

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

Membros

Presidente da Comissão / Representante da DGTI

Francisco Hamilton de Freitas Júnior

Representante da Reitoria

Douglas Iuri Medeiro Cabral

Leonardo Ferreira Cavalcanti

Sérgio Manuel Pão-Mole Bento

Representante do Campus Petrolina

Andson da Silva Rodrigues

Cleiton Rodrigues de Souza

Lucas Souza Santo

Melquizedequi Cabral dos Santos

Natalia Rafaela Nascimento da Silva

Representante do Campus Petrolina Zona Rural

Milton Deivson Albuquerque Cavalcante

Tarcisio Couto Pereira

Vandenberg Borges da Paixão

Representante do Campus Ouricuri

Joana Darc Quesado Oliveira

Antonio Jelson Bezerra Lopes

Representante do Campus Serra Talhada

Danyel Mendes Nogueira Ramos

Representante do Campus Floresta

Danilo Rosa Quirino de Sa

Vagner de Souza Alves

Representante do Campus Salgueiro

Antônio Epaminondas Sobreira Honorato

Wiharlley Moises Santos Alves

CONTROLE DO DOCUMENTO

- **Armazenamento do Documento**

Título do Documento	Política de Segurança da Informação e Comunicação
Localização do Documento	http://www.ifsertao-pe.edu.br/dgti/index.php/documentos-oficiais
Formato do Documento	PDF

- **Aprovações**

Nome	**Cargo**	**Data da Aprovação**	**Versão Aprovada**
Sebastiao Rildo Fernandes Diniz	Reitor (a)	17/04/2012	1.0
Sebastiao Rildo Fernandes Diniz	Reitor (a)	09/09/2013	1.1
Maria Leopoldina Veras Camelo	Reitor (a)	12 / 08 / 2016	1.2

CAPITULO I

1 – VISÃO GERAL

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

A proposta desta Política de Segurança da Informação e Comunicação (POSIC) é estabelecer as diretrizes para a proteção dos ativos de informação do IF SERTÃO-PE. Esse documento contem diretrizes gerais de segurança e controle de proteção da informação. Tais controles são descritos e padronizados pelos processos e procedimentos de segurança da informação com ferramentas e conscientizações.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos usuários, quando na utilização dos recursos de processamento da informação do IF SERTÃO-PE.

2 – OBJETIVO E METAS

Regularizar e normatizar o uso dos recursos e serviços prestados pelos setores de Tecnologia da Informação (TI) da Reitoria e de todos os *Campi* da instituição. Visando atingir as seguintes metas:

2.1 - Melhoria da segurança dos usuários online;

2.2 - Melhorias da segurança dos meios de comunicação de dados ;

2.3 - Melhoria da segurança dos sistemas computacionais.

3 – ESCOPO

A POSIC se aplica a todos os colaboradores, empresas terceiras ou agentes que possuem acesso às informações do IF SERTÃO-PE.

A POSIC se aplica a todas as formas de informação, incluindo:

3.1 - Dados impressos, manuscritos ou armazenamentos digitalmente;

3.2 - Correios eletrônicos;

3.3 - Processadas por computadores ou dispositivos eletrônicos quaisquer;

3.4 - Discussões, reuniões, comunicados executados por qualquer meio de comunicação digital.

4 - INSTÂNCIAS ADMINISTRATIVAS

Para os efeitos desta política e das normas nela originadas, entende-se por:

4.1 - **Políticas de Segurança da Informação e Comunicações (POSIC)-** Documento aprovado pela autoridade máxima do órgão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficiente à implementação da segurança da informação e comunicações;

4.2 - **Comitê Gestor de Segurança da Informação (CGSI):** comitê responsável por elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicação (POSIC) e normas relacionadas, submetendo à aprovação do Conselho superior do IF Sertão-PE, entre outras competências;

4.3 - **Diretoria de Gestão Tecnologia da Informação (DGTI):** órgão executivo da Pró-reitora de Desenvolvimento Institucional (PRODI), que planeja, dirige, avalia e executa as políticas de tecnologia da informação comunicação (TIC) em todo o Instituto, em articulação com as Pró-reitoras e as Direções Gerais dos Campi.

5 – CONCEITOS E DEFINIÇÕES

5.1 - **Ativo de informação:** qualquer informação que tenha valor para a Instituição, nos termos da Norma ISO/IEC nº 13335-1:2004;

5.2 - **Recursos de processamento da informação:** qualquer sistema, serviço ou infraestrutura de processamento da informação, ou as instalações físicas que os abriguem;

5.3 - **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;

5.4 - **Incidente de segurança da informação:** ocorrência indicada por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que apresentem grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação, nos termos da Norma ISO/IEC TR nº 18044:2004;

5.5 - **Ameaça**: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição, nos termos da Norma ISO/IEC nº 13335-1:2004;

5.6 - **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

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

5.8 - **Plano de continuidade de negócios:** conjunto de procedimentos a serem adotados quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços;

5.9 - **Princípios da Segurança da Informação e Comunicações**: princípios que regem a Segurança da Informação e Comunicações, nos termos do art. 3° do Decreto n° 3.505, de 13 de junho de 2000, ou seja, a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio;

5.10 - **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;

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

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

5.13 - **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;

5.14 - **Gestão da continuidade de negócios:** processo contínuo de gestão e governança, suportado pela alta direção, com recursos apropriados para garantir que as ações necessárias sejam executadas de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento dos serviços;

5.15 - **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar seu risco;

5.16 - **Avaliação de riscos:** processo por intermédio do qual se compara o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;

5.17 - **Gestão de Riscos de Segurança da Informação e Comunicação:** conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias, especificamente, para mitigar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

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

5.19 - **Tratamento dos riscos:** processo de implementação de ações de Segurança da Informação e Comunicações destinadas a evitar, reduzir, reter ou transferir um risco;

5.20 - **Gestor**: agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas de uso da informação;

5.21 - **Usuário interno:** qualquer pessoa física ou unidade interna que faça uso de informações e/ou equipamentos que estejam vinculados administrativamente ao do IF SERTÃO-PE;

5.22 - **Usuário externo:** qualquer pessoa física ou jurídica que faça uso de informações e/ou equipamentos que não esteja vinculada administrativamente ao IF SERTÃO-PE;

5.24 - **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;

5.25 - **Comunicação informal:** tráfego de documentos, informações ou formulários que não estejam incluídos no conceito de que trata o inciso anterior, emitidos via caixas postais eletrônicas individuais de autoridade, servidor, estagiário ou fornecedor de bens e/ou serviços.

6 - DIRETRIZES GERAIS

6.1 - Cada servidor público é responsável pela Segurança da Informação dentro do IF SERTÃO-PE, principalmente pelas informações que estão sob sua responsabilidade;

6.2 - O IF Sertão-PE, como usuário dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança;

6.3 - Os usuários internos e externos devem observar que:

6.3.1 - 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;

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

6.3.3 - As normas para as operações de armazenamento, divulgação, reprodução, recuperação e destruição da informação serão definidos de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor;

6.4 - 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 informal. O correio eletrônico constitui bem do IF Sertão-PE e, portanto, passível de auditoria;

6.5 - O acesso à Internet será concedido para todos os servidores, com utilização exclusiva para fins diretos e complementares às atividades do setor;

6.6 - O acesso à Internet será concedido para todos os alunos com utilização para fins acadêmicos E/OU ATIVIDADES QUE NÃO INFRINJA A ESTA POSIC;

6.7 - Todo acesso à Internet será monitorado e passível de auditoria.

7 – DAS RESPONSABILIDADES E COMPETÊNCIAS

7.1 - A responsabilidade pela segurança das informações deverá esta estabelecida nos documentos oficiais do IF SERTÃO-PE e principalmente na Politica de Segurança da Informação;

7.2 - O monitoramento do uso da internet é importante para que sejam registrados todos os acessos de cada usuário e para que possam ser notificados e até mesmo punidos nos casos de acesso que sejam contrários a política do IF SERTÃO-PE;

7.3 - São responsabilidades dos usuários de serviços de redes de dados, internet, correio eletrônico e/ou outros recursos computacionais oferecidos pelo IF SERTÃO-PE:

7.3.1 - Promover a segurança do seu usuário corporativo, bem como suas respectivas senhas;

7.3.2 A identificação do usuário por meio de senha é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela;

7.3.3 Seguir de forma colaborativa as orientações fornecidas pelos setores competentes em relação ao melhor uso dos recursos computacionais, de rede de dados, internet, telecomunicações e correio;

7.3.4 - Utilizar de forma ética e legal os recursos computacionais, de rede de dados, internet, telecomunicações e correio eletrônico;

7.4 - Compete à Diretoria de Gestão e Tecnologia da Informação zelar pela segurança da informação no âmbito do IF SERTÃO-PE quando as informações estiverem sobcustódia dos recursos de tecnologia da informação.

7.5 - Compete aos Setores de Tecnologia da Informação dos campi zelar pela segurança da informação no âmbito de cada campus quando as informações estiverem sob custódia dos recursos de tecnologia da informação.

7.6 - A implementação, o controle e a gestão da POSIC observarão a seguinte estrutura de gerenciamento:

7.6.1 - A autoridade máxima do IF SERTÃO-PE é o Conselho Superior, responsável pela aprovação da POSIC;

7.6.2 Ao Comitê Gestor de Segurança da Informação compete:

a) Promover a cultura de Segurança da Informação;

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) Propor recursos necessários às ações de Segurança da Informação;

d) Realizar e acompanhar estudos de novas tecnologias, no que diz respeito a possíveis impactos sobre a Segurança da Informação;

e) Coordenar as revisões das normas de segurança em vigor;

f) Fazer trabalho de conscientização, educação e treinamento da segurança da informação no âmbito do IFSERTAO-PE;

g) Acordar sobre papéis e responsabilidades específicas para segurança de informações em toda a organização;

h) Acordar sobre metodologias e processos específicos para segurança de informações;

i) Apoiar iniciativas de segurança de informação que abrangem toda a organização. Por exemplo: programas de conscientização sobre segurança;

j) Promover a visibilidade do suporte corporativo para a segurança de informações em toda a organização.

8– DAS FUNDAMENTAÇÔES LEGAIS E NORMATIVAS

8.1- Constituição Federal de 1988;

8.2 - Norma ABNT NBR ISO nº 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;

8.3- Norma ABNT NBR ISO/IEC nº 27001:2005: Tecnologia da Informação – Técnicas de Segurança– Sistemas de Gerência da Segurança da Informação – Requisitos;

8.4 - Normas ABNT NBR ISO/IEC 27002:2005 – Técnicas de segurança – Código de práticas para a segurança da informação;

8.5 - Norma ISO/IEC TR nº 13335-3:1998, que fornece técnicas para a gestão de segurança na área de tecnologia da informação, baseada nas normas ISO/IEC nº 13335-1 e TR ISO/IEC nº 13335-2;

8.6 - Conforme o 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.

8.7 – Lei nº 8.112 de 11 de dezembro de 1990 - Regime jurídico dos servidores públicos civil da União, das autarquias e das fundações públicas federais;

8.8 - Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto Lei nº 2848/40 (Código Penal Brasileiro), de modo a prever a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

8.9 - Decreto nº 1.171, de 24 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

8.10 – Outros dispositivos legais aplicáveis, a saber:

8.10.1 - Norma Complementar nº 01/IN01/DSIC/GSIPR, de 13 de outubro de 2008;

8.10.2 - Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 de outubro de 2008;

8.10.3 - Norma Complementar nº 03/IN01/DSIC/GSIPR, de 3 de julho de 2009;

8.10.4 - Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 de agosto de 2009;

8.10.5 - Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;

8.10.6 - Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;

8.11 - Lei nº 7.232, de 29 de outubro de 1984, que dispõe sobre a Política Nacional de Informática;

8.12 - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

8.13 - 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;

8.14 - Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

9 - DA DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

A alta direção IF SERTÃO-PE, na figura do Reitor, declara-se comprometida em proteger todos os seus ativos de informação.

10 - VIOLAÇÕES, PENALIDADES E SANÇÕES

Nos casos em que houver o descumprimento ou violação de um ou mais itens da Política ou de seus regulamentos, procedimentos ou atividades pertinentes à Segurança da Informação, estes serão tratados individualmente em cada capitulo.

11 – PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

11.1 - Esta Política abrange onze aspectos básicos da Segurança da Informação e Comunicações, destacados a seguir:

11.1.1 - **Confidencialidade**: somente pessoas devidamente autorizadas pelo gestor da informação devem ter acesso à informação não pública;

11.1.2 – **Integridade**: somente operações de alteração, supressão e adição autorizadas pelo IFSERTÃO-PE de vem ser realizadas nas informações;

11.1.3 – **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

11.1.4 – **Autenticidade**: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

11.1.5 – **Criticidade**: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

11.1.6 – **Não Repúdio:** garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo sua identificação;

11.1.7 - **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 IF SERTÃO-PE são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação advindas desta Política;

11.1.8 – **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;

11.1.9 – **Ética**: todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, presta dores de serviço e usuários do sistema de Informação do IFSERTÃO-PE devem ser respeitados;

11.1.10 – **Legalidade**: além de observar os interesses do IF Sertão-PE, 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 aos direitos de uso;

11.1.11 – **Proporcionalidade**: o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no âmbito IF SERTÃO-PE serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

12 – ABRANGÊNCIA

Essa norma se aplica em todo âmbito do Instituto Federal do Sertão Pernambucano.

13 – REVISÃO E ATUALIZAÇÃO

A política PODERÁ ser atualizada sempre que uma nova tecnologia surgir, instruções normativas existentes sofrerem alterações ou conforme necessidade do CGSI. Deverá ser revisada anualmente ou conforme necessidade do CGSI.

14 - ORIGEM

Diretoria de Gestão de Tecnologia da Informação

CAPITULO II

Regulamenta o uso do e-mail institucional

TÍTULO I

DO OBJETIVO

Art. 1° Esta regulamentação tem por objetivo estabelecer padrões, responsabilidades e requisitos básicos de utilização do e-mail institucional no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – IF SERTÃO-PE.

TÍTULO II

DO CAMPO DE APLICAÇÃO

Art. 2° As diretrizes estabelecidas no presente documento deverão ser aplicadas em todos os Campi que compõe o IF – IF SERTÃO-PE, bem como na Reitoria.

TÍTULO III

DAS DEFINIÇÕES

Art. 3° Para os fins desta Instrução Normativa devem ser adotadas as seguintes definições:

I. **Webmail** – Interface da Wold Wide Web que permite ao utilizador ler e escrever e-mail usando um navegador.

II. **Brower** - Também conhecido como navegador. É um programa de computador que habilita seus usuários a interagirem com documentos virtuais da Internet, também conhecidos como páginas da web.

III. **Correio Eletrônico** – Correio eletrônico (português brasileiro) ou e-mail é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.

IV. **Servidor de Correio Eletrônico** – Hardware com configuração específica para implantar um sistema de Correio Eletrônico.

V. **Matrícula Siape** – Número único de identificação dos servidores públicos federal.

TÍTULO IV

DOS CONCEITOS

Art. 4° Entende-se por e-mail institucional o serviço de comunicação via mensagens entre usuários de uma corporação através da Internet, utilizando-se de tecnologias específicas para tal. O e-mail institucional é de extrema importância dentro da instituição, visto que facilita o tráfego de informação dentro da mesma.

TÍTULO V

DAS NORMAS PARA UTILIZAÇÃO DO E-MAIL INSTITUCIONAL

Art. 5° O serviço de e-mail institucional será fornecido por um servidor de correio eletrônico próprio, localizado nas dependências da instituição.

Art. 6° O e-mail institucional será fornecido pelo – IF SERTÃO-PE a todos os servidores públicos da instituição.

Parágrafo único. A criação de conta de e-mail institucional será realizada somente com a posse do número de matrícula do SIAPE do servidor.

Art. 7º As contas de e-mail institucional serão de dois tipos: Conta do Servidor e Conta de Departamento ou Serviço/Evento.

§ 1º Conta de Servidor é a conta de e-mail vinculada ao servidor público do – IF SERTÃO-PE.

§ 2º Conta do Servidor e Conta de Departamento ou Serviço/Evento é a conta de e-mail vinculada a um departamento, serviço ou evento da instituição, juntamente com o chefe e seus subordinados.

§ 3º Listas são os e-mails nos quais estão vinculadas diversas contas institucionais conforme um determinado grupo. Ex.: listas de e-mails administrativos; lista de e-mails de docentes.

Parágrafo Único: os e-mails do tipo Lista somente aceitam mensagens de e-mails que sejam originados no próprio e-mail institucional, portanto não recebem mensagens de serviços de e-mails externos.

Art. 8º O acesso às contas de e-mail será realizado somente via webmail, através de um browser.

Art. 9º Compete à DGP ou SGP solicitar a criação da conta de e-mail institucional de um servidor.
Art. 10 º Compete ao chefe de departamento solicitar a criação da conta institucional vinculada ao departamento, bem como vincular e desvincular usuários a esta conta.

Art. 11 º Compete ao presidente da portaria solicitar a criação da conta institucional vinculada a um grupo, bem como vincular e desvincular usuários a esta conta.

Art. 12 º Compete a Diretoria de Gestão de Pessoas informarem sobre o desligamento de um servidor da instituição para que seja desativada sua conta de e-mail ou o próprio usuário também pode solicitar a desativação da conta em virtude de desligamento da instituição, a solicitação deverá ser encaminhada ao endereço **webmail@ifsertao-pe.edu.br**.

Parágrafo único. O servidor desligado do – IF SERTÃO-PE terá um período de 90 dias para reencaminhar suas mensagens para outra conta de e-mail, após este período, sua conta será excluída permanentemente.

Art. 13° O espaço inicial da caixa de e-mail institucional será de 200 MB.

Parágrafo único. Compete ao responsável pela conta solicitar aumento de sua caixa de e-mail, quando necessário, justificando-o. A solicitação deverá ser encaminhada ao endereço webmail@ifsertao-pe.edu.br.

TÍTULO VI

DA FORMATAÇÃO DE CONTAS DO E-MAIL INSTITUCIONAL

Art. 14° As contas dos servidores públicos ativos deverão obedecer a seguinte formatação: nome.sobrenome@ifsertao-pe.edu.br

Parágrafo único. As contas de usuário individual criadas para os servidores são de responsabilidade destes, que assinarão formalmente um termo de responsabilidade durante a vigência da respectiva conta.

Art. 15° A identificação dos departamentos terá o prefixo de identificação do *campus* ao qual pertença, sendo assim identificados:

I – CP- *Campus* Petrolina

II – CF – *Campus* Floresta

III – CS – *Campus* Salgueiro

IV – CO – *Campus* Ouricuri

V- CZR – *Campus* Petrolina Zona Rural

VI – RT- Reitoria

VII – CST - Serra Talhada

VIII – CSMBV - Santa Maria da Boa Vista

§ 1º - As contas dos departamentos deverão obedecer à seguinte formatação: prefixo do campus.departamento@ifsertao-pe.edu.br

§ 2º As contas de usuário institucionais criadas para os Setores, Diretorias e Pró-Reitorias são de responsabilidade dos titulares das respectivas funções, que assinarão formalmente um termo de responsabilidade durante a vigência da respectiva conta.

§ 3º Os Departamentos que existem apenas na Reitoria e os sistemas que sejam de âmbito do IF SERTÃO-PE, como Pró-Reitorias, Diretorias Sistêmicas, Concurso Público e Exame Seletivo não precisam utilizar o prefixo.

§ 4º Na criação de novos campi, também será utilizada a identificação dos departamentos através de prefixo.

Art. 16 As contas dos serviços devem ter o prefixo do campus seguido da identificação do serviço:

Ex: cp.gispe@ifsertao-pe.edu.br, cp.cci@ifsertao-pe.edu.br.

Art. 17° As contas de eventos temporários devem conter o prefixo do campus, identificar o evento e ficarão válidas pelo tempo de divulgação até a data de finalização do mesmo, determinada pela coordenação do evento.

Ex: cp.snct2011@ifsertao-pe.edu.br.

Parágrafo único. As contas de eventos temporários ficarão válidas até o término do evento.

TÍTULO VII

DOS DEVERES E RESPONSABILIDADES DO USUÁRIO

Art. 18° São deveres do usuário individual ou institucional:

I - Manter em sigilo sua senha de acesso ao correio eletrônico, visto que esta senha é de uso pessoal e intransferível, realizando a substituição desta em caso de suspeita de violação;

II - fechar a página de acesso do e-mail institucional toda vez que se ausentar, evitando o acesso indevido;

III - comunicar, imediatamente, ao administrador de contas de e-mail, do recebimento de mensagens com vírus, spam, ou qualquer outro tipo de conteúdo inadequado;

IV - efetuar a manutenção de sua Caixa Postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo;

V - notificar o administrador de contas de e-mail quando ocorrerem alterações que venham a afetar o cadastro do usuário de e-mail;

VI – toda alteração ou demanda nas contas de e-mail deverão ser solicitadas através do endereço webmail@ifsertao-pe.edu.br.

Art. 19° São deveres dos usuários dos grupos de e-mail:

I. Utilizar a ferramenta de distribuição de mensagens exclusivamente para troca de mensagens que sejam de interesse institucional ou do grupo;

II. Não permitir acesso de terceiros às listas de distribuição de e-mail;

III. Guardar sigilo funcional sobre as discussões travadas nos respectivos grupos;

IV. Notificar ao administrador de contas de e-mail quando do recebimento de mensagens que contrariem o disposto nesta regulamentação.

Art. 20° São deveres do administrador das contas de e-mail:

I. Disponibilizar a utilização do e-mail institucional aos servidores do – IF SERTÃO-PE, reservando-se no direito de, a seu livre critério, fixar limites quanto ao tamanho das caixas postais, volume total de mensagens enviadas, quantidade de mensagens armazenadas nos servidores de e-mail, número de destinatários e tamanho de cada mensagem enviada;

II. Informar aos demais servidores do – IF SERTÃO-PE sobre interrupções previsíveis desses serviços;

III. Prestar esclarecimentos aos servidores do IF SERTÃO-PE, quando solicitado, em relação ao uso do e-mail institucional e demais aplicativos constantes na página de correio eletrônico;

IV. Alterar senha para acesso ao e-mail institucional;

V. gerar e manter grupos e listas de discussão mediante solicitação formal;

VI. Administrar e programar políticas, procedimentos e melhores práticas relativos aos serviços de e-mail institucional, zelando pelo cumprimento de leis e normas aplicáveis;

VII. Verificar periodicamente o desempenho, a disponibilidade e a integridade do sistema de e-mail institucional;

VIII. Estabelecer procedimentos e rotinas de manutenção de contas de e-mail institucional;

IX – manter sigilo sobre as correspondências bem como protegê-las contra ataques e invasões.

TÍTULO VIII

DAS CONDIÇÕES GERAIS DE UTILIZAÇÃO

Art. 21° São condições gerais de utilização do e-mail institucional:

I - Veiculação de mensagens de conteúdo, exclusivamente, acadêmico ou administrativo; não sendo permitido o uso para fins comerciais, políticos, religiosos, enfim, que não seja consonante com o uso institucional;

II - As mensagens emitidas através do e-mail institucional são elementos de formação da imagem institucional do – IF SERTÃO-PE, portanto, devem merecer o mesmo tratamento da correspondência impressa;

III - É inadmissível o uso do e-mail institucional do – IF SERTÃO-PE para transmissão e recebimento de mensagens pessoais do usuário individual, bem como para acesso a redes sociais, cadastros em sites de compras bem como qualquer outra utilização estranha às funções institucionais / funcionais.

IV - é vedada a cessão, a qualquer título, da lista de endereços dos usuários do e-mail institucional do Instituto à pessoa estranha aos quadros do – IF SERTÃO-PE, salvo para finalidade institucional;

V - a Diretoria de Gestão de Tecnologia da Informação não se obriga a garantir a inviolabilidade absoluta das mensagens eletrônicas que trafegarem no e-mail institucional.

Art. 22° É considerado uso indevido do Correio Eletrônico:

I - Tentar acessar as caixas postais de terceiros sem autorização;

II - enviar informações sensíveis, classificadas ou proprietárias, inclusive senhas, para pessoas ou organizações não autorizadas;

III - enviar material obsceno, ilegal ou não ético, comercial, estritamente pessoal, de propaganda, mensagens do tipo corrente, entretenimento, "spam" (envio de mensagem não solicitada), propaganda política e "hoax" (mensagens enganosas);

IV - enviar mensagens ofensivas que visem atingir a honra e/ou a dignidade das pessoas;

V - enviar música, vídeos ou animações que não sejam de interesse específico do trabalho;

VI - enviar mensagens contendo vírus ou qualquer forma de rotinas de programação prejudiciais ou danosas às estações de trabalho e ao sistema de e-mail de forma proposital;

VII - forjar a identidade de outra pessoa (por exemplo, usando o endereço de e-mail dessa pessoa) ou fazer falsa declaração de sua identidade ou da fonte de qualquer e-mail;

VIII - transmitir ilegalmente propriedade intelectual de terceiros ou outros tipos de informações proprietárias sem a permissão do proprietário ou do licenciante;

IX - usar o e-mail institucional para violar direitos;

X - promover ou incentivar atividades ilícitas;

XI - vender, comprar, negociar, revender, transferir ou de alguma forma explorar para fins comerciais não autorizados qualquer Conta do e-mail institucional;

XII - modificar, adaptar, traduzir ou fazer engenharia reversa de qualquer parte do serviço de e-mail institucional;

XIII - reformatar qualquer página da web que faça parte do serviço de e-mail institucional;

XIV - usar o serviço de e-mail institucional em associação ao compartilhamento ilegal de arquivos ponto-a-ponto;

XV - outras atividades que possam afetar, negativamente, o – IF SERTÃO-PE, servidores ou terceiros, e que não tenham finalidade amparada pela legislação.

§1º Caso ocorra constatação de má utilização do e-mail institucional, a Diretoria de Gestão de Tecnologia da Informação reserva-se o direito de investigar o acesso do usuário ao Correio Eletrônico.

§ 2º A Diretoria de Gestão de Tecnologia da Informação poderá suspender o acesso do usuário à rede e ao e-mail institucional em caso da comprovação de utilização inadequada.

Art. 23° O usuário não deverá enviar e-mail com anexo que excedam 9 MB.

Parágrafo Único – Arquivos anexos nas mensagens recebidas poderão ser bloqueados de acordo com a sua extensão (tipo de arquivo) e/ou seu tamanho, como forma de garantir a segurança da rede e a capacidade das máquinas servidoras.

Art. 24° O usuário deverá utilizar o campo "CCO" para enviar mensagens quando a quantidade de destinatários for superior a 5 (cinco).

TÍTULO IX

DAS RECOMENDAÇÕES

Art. 25° É recomendado ao usuário do e-mail institucional:

I – Ao enviar e-mail com anexos faça uso de ferramentas de compactação de arquivos ou arquivos de formato reduzidos (. zip .rar,.pdf,.jpg,entre outros);

II – não responder e-mail incluindo os anexos recebidos;

III – não enviar e-mail com arquivos anexos às listas de e-mail;

IV – apagar e-mail desnecessário e, principalmente, os que possuem anexos;

V – não responder ou abrir e-mail cujo remetente e/ou conteúdo da mensagem sejam desconhecidos ou de caráter duvidoso;

VI – apagar mensagens com conteúdo e anexos duvidosos;

VII – informar à DGTI sobre o recebimento constante de e-mail não solicitado por parte do usuário;

VIII – informar à DGTI sobre qualquer ação suspeita que venha ocorrer com sua conta de e-mail.

TÍTULO X

DAS INFRAÇÕES

Art. 26° Serão consideradas infrações:

I – Fornecer a senha de acesso a terceiros;

II – utilizar os recursos oferecidos com fins comerciais ou para benefício próprio;

III – utilizar software ou procedimentos para conseguir acesso não autorizado a recursos ou informações, ou para degradar o desempenho, ou para colocar fora de operação sistemas computacionais locais ou remotos;

IV – armazenar arquivos de conteúdo ilegal ou considerados abusivos;

V – manter comportamento ofensivo ou impróprio no tratamento com outros usuários ou grupos – local ou externo.

VI – utilizar recursos do e-mail para envio de spam, correntes, boatos e afins;

VII – envolver-se em qualquer atividade que infrinja ou boicote a política de segurança;

VIII – utilizar o e-mail para divulgar, propagar ou guardar vírus ou qualquer outro tipo de programa nocivo, bem como material protegido por leis de propriedade intelectual;

IX – violar outras regras e diretrizes de usuários ou administrador previstas nos documentos da "Política de Segurança de TI do IF SERTÃO-PE".

TÍTULO XI

DAS PENALIDADES

Art. 27° Os usuários das contas de e-mail institucional do IF Sertão-PE que o utilizarem incorretamente, infringindo as disposições mencionadas nesta regulamentação, estarão sujeitos às seguintes consequências, sem prejuízo de suas responsabilidades, direitos, deveres e proibições:

I – O usuário será comunicado por escrito (via e-mail ou manual);

II – em caso de reincidência, a chefia imediata será comunicada (via e-mail ou manual);

III – persistindo a infração, haverá restrição dos serviços (bloqueio da conta do usuário por tempo indeterminado); e será encaminhada ao Reitor para fazer a notificação à Comissão de Ética IF SERTÃO-PE, solicitando apuração da eventual responsabilidade.

TÍTULO XII

DISPOSIÇÕES FINAIS

Art. 28° Esta regulamentação entra em vigor na data de sua publicação.

Art. 29°. Os casos omissos serão dirimidos pelo Comitê Gestor de Tecnologia da Informação.

CAPITULO III

Regulamenta a utilização da Internet

TÍTULO I

DO OBJETIVO

Art. 1° Esta regulamentação tem por objetivo estabelecer responsabilidades e requisitos básicos de utilização da Internet no Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – IF SERTÃO-PE.

TÍTULO II

DO CAMPO DE APLICAÇÃO

Art. 2° As diretrizes estabelecidas no presente documento deverão ser aplicadas em todos os *Campi* que compõe o IF SERTÃO-PE, bem como na Reitoria.

TÍTULO III

DAS DEFINIÇÕES

Art. 3° Para os fins desta Instrução Normativa devem ser adotadas as seguintes definições:

I. **Download**– Descarregamento, transferência de arquivo entre computadores por meio de uma rede.

II. **Hacker** - Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.

III. **Upload** – Envio de um arquivo do seu computador para outro, através da Internet.

IV. **Peer-to-Peer (P2P) –** Rede computacional descentralizada onde cada computador pode funcionar como servidor (fornecendo dados) e como cliente (recebendo). É mais comumente usada para designar programas de compartilhamento de arquivos entre usuários.

V. **Site –** Páginas contendo conteúdo dinâmico OU ESTÁTICO como informações, imagens, fotos, vídeos, sons, etc., que ficam armazenadas em provedores de acesso (computadores denominado servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte a rede.

TÍTULO IV

DOS CONCEITOS

Art. 4° Entende-se por acesso e uso da Internet os serviços oferecidos na Rede Mundial de Computadores.

Parágrafo Único. Todos os usuários que utilizarem o serviço deverão fazê-lo no interesse da Instituição, mantendo uma conduta profissional.

TÍTULO V

DAS NORMAS PARA UTILIZAÇÃO DA INTERNET

Art. 5° Serão considerados usos indevidos, abusivos ou excessivos no uso da Internet:

I – Acesso a portais ou páginas inseguras e sem certificado de segurança, que ofereçam riscos de contaminação por vírus ou por outro código nocivo de programação no ambiente de rede corporativa.

II – Arquivos que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos.

III – Sites que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos.

IV – Acesso a sites de relacionamento tais como Badoo, facebook, entre outros, podendo ser desbloqueados de acordo com a necessidade da Instituição.

V – Acesso a sites com conteúdo pornográfico, pedófilo, erótico, racista, entre outros.

VI – Site com conteúdo impróprio, ofensivo, ilegal, discriminatório e similar.

VII – Acesso a sites de jogos on-line com intuito de interagir com os mesmos (jogar), sem finalidade acadêmica e/ou institucional.

§ 1º O acesso a sites com conteúdo pornográfico, pedófilo, erótico, racista serão bloqueados e as tentativas de acesso serão monitoradas.

§ 2º Haverá geração de relatórios gerenciais para identificação de abusos e mau uso dos recursos acessados.

§ 3º O fato de um site não estar bloqueado, não significa que o mesmo possa ser acessado pelo usuário.

§ 4 Caso seja necessário, haverá publicação dos relatórios e prestação de contas dos acessos do usuário.

Art. 6º Para usar a internet sem fio na Reitoria ou no *Campus* é necessário cadastrar o usuário e o equipamento junto à Diretoria de Gestão de Tecnologia da Informação (DGTI) ou Coordenação de Informática.

Parágrafo único. Será criado um login e uma senha, de uso pessoal e intransferível.

TÍTULO VI

DAS PROIBIÇÕES

Art. 7° É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas corporativas em lista de discussão ou bate-papo, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei.

Art. 8º Não será permitida a utilização de softwares de peer-to-peer (P2P), tais como Kazaa, Bit, Torrent, Emule e afins.

Art. 9º É proibido utilizar os recursos da rede para fazer download de software pirata, ou dado não legalizado.

Art. 10º Não será permitida a utilização de serviços de streaming, tais como Rádios on-line, vídeos e afins, desde que não seja de interesse da Instituição.

Art. 11º Não será permitido o uso de serviços de anonimato para acesso à Internet (Ex.: ultrasurf).

Art. 12º É proibido o uso da Internet para fins comerciais.

TÍTULO VII

DAS RESPONSABILIDADES

Art. 13º O gerenciamento e manutenção dos serviços da Internet são de responsabilidade das Coordenações de Informática de cada *Campus*, juntamente com a Diretoria de Gestão de Tecnologia da Informação (DGTI).

Art. 14º O usuário é pessoalmente responsável por todas as atividades realizadas.

Art. 15º Todos os usuários estão sujeitos à auditoria em sua utilização dos recursos, com o objetivo de observar o cumprimento desta resolução pelos usuários e com vistas à gestão de desempenho de segurança.

Art.16 º Reserva-se o direito às Coordenações de Informática dos Campi e à DGTI de monitorar o tráfego efetuado através de suas redes de comunicação, incluindo o acesso à Internet, para verificar o cumprimento das normas.

TÍTULO VIII

DAS PENALIDADES

Art. 17º Aos alunos, terceirizados ou estagiários que violarem qualquer item desta norma de segurança, terão sua permissão de acesso à Internet bloqueada, será notificado a Direção de Ensino ou ao setor responsável para que sejam tomadas as providências.

Art. 18º Quando se tratar de servidor da Instituição, o mesmo será notificado, via e-mail, do descumprimento das normas estabelecidas.

§ 1º Persistindo a infração da norma, o servidor será novamente notificado, via e-mail, e será encaminhada cópia da notificação para sua chefia imediata, Diretor do Campus ou, quando se tratar de servidor lotado na Reitoria, a notificação será encaminhado ao Pró-Reitor responsável ou Reitor ao qual conduzirá a abertura de um processo administrativo prevista na lei 8112 para apuração e responsabilidade pelas violações da norma de segurança.

TÍTULO IX

DAS PENALIDADES ESPECIAIS

Art. 19º Será aberto inquérito na delegacia da Polícia Federal, quando o usuário insistir em acessar sites que tiverem conteúdo de pedofilia, racismo ou qualquer outro assunto contrário à Lei e que eventualmente não esteja bloqueado no sistema de proteção.

TÍTULO X

DISPOSIÇÕES FINAIS

Art. 20º Esta regulamentação entra em vigor na data de sua publicação.

Art. 21º. Os casos omissos serão dirimidos pelo Comitê Gestor de Tecnologia da Informação

CAPITULO IV

Regulamenta a utilização das estações de trabalho em rede

TÍTULO I

DO OBJETIVO

Art. 1° Esta regulamentação tem por objetivo estabelecer normas para utilização de estação de trabalho na rede corporativa do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – IF SERTÃO-PE.

TÍTULO II

DO CAMPO DE APLICAÇÃO

Art. 2° As diretrizes estabelecidas no presente documento deverão ser aplicadas em todos os *Campi* que compõe o IF SERTÃO-PE, bem como na Reitoria.

TÍTULO III

DAS DEFINIÇÕES

Art. 3° Para os fins desta Instrução Normativa devem ser adotadas as seguintes definições:

I. **Tokens** – Dispositivo físico para autenticações

II. **Helpdesk** - Fone de suporte técnico para usuários.

III. **Login** – Processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema.

IV. **Usuário** – Pessoa que utiliza algum recurso ou serviço de tecnologia da informação.

V. **Conta de Usuário** – Identificação de um usuário para acesso a algum recurso ou serviço da rede.

VI. **Estação de Trabalho** – Computador que fornece serviços a uma rede de computadores (Ex. Internet, Correio eletrônico, banco de dados, etc.).

VII. **Privilégio de Administrador** – Pessoas com permissão para realizar certas ações nos computadores institucionais e na rede, como, por exemplo, instalação de programas.

VIII. **Backup** - Cópia de segurança (em inglês: backup) é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

TÍTULO IV

DOS CONCEITOS

Art. 4° As estações de trabalho possuem informações que permitem que sejam identificadas na rede.

Parágrafo único. Cada usuário possui seu próprio login para acesso aos recursos da rede.

TÍTULO V

DAS NORMAS PARA UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO EM REDE

Art. 5° Todo computador do IF SERTÃO-PE receberá um nome exclusivo que o identificará na rede corporativa.

Art. 6° O nome do computador iniciará com o acrônimo que identifica o *campus* de origem da máquina.

I – CPE- *Campus* Petrolina

II – CFL – *Campus* Floresta

III – CSA – *Campus* Salgueiro

IV – COU – *Campus* Ouricuri

V- CZR – *Campus* Petrolina Zona Rural

VI – REI- Reitoria

VII – CST – Campus Serra Talhada

VIII – CSMBV – Campus Santa Maria da Boa Vista

§ 1º Após as iniciais que identifica o campus, seguido do símbolo " - ", seguirá a sigla do setor onde a máquina será instalada.

§ 2º Será acrescentado um número com 5 algarismo que identificará o tombo da máquina (Ex.: REI-DGTI-12385, onde, REI = Reitoria, DGTI = Diretoria de Gestão da Tecnologia da Informação e 12345 = Tombo)

Art. 7º Todas as formas de acesso, redes, estações de trabalho e sistemas poderão ser passíveis de auditorias de TI.

Parágrafo único. As Coordenações de TI dos *Campi* e a DGTI auditarão, regularmente, o uso dos recursos e serviços de TI do IF SERTÃO-PE de modo a salvaguardar os interesses da Instituição, no que diz respeito à segurança das informações, bem como o uso adequado dos recursos de TI.

Art. 8º A Instituição não se responsabilizará pelos arquivos armazenados nos discos rígidos locais.

§ 1º É de inteira responsabilidade do usuário, fazer backup dos seus arquivos.

§2º O usuário deve fazer manutenção no diretório pessoal, evitando acúmulo de arquivos desnecessários.

Art. 9º O acesso a sistemas e demais recursos de TI, sempre que possível, deve ser controlado pela identificação do usuário (login).

Art. 10º O IF SERTÃO-PE não fornecerá acessórios, software ou suporte técnico para equipamento de informática particular – computadores, impressoras, notebook, entre outros.

Art. 11º Toda solicitação de suporte (instalação, prevenção e correção) pelo usuário deverá ser feita através de um serviço Web para abertura e acompanhamento de chamados, atendendo a ordem de prioridade, desde que a rede interna e/ou externa esteja em funcionando.

Art. 12º Em caso de exoneração de servidor, a Diretoria de Gestão de Pessoas – DGP, deverá solicitar ao setor de TI a desativação da conta de usuário e de todos os acessos do usuário exonerado (e-mail, rede e sistemas).

Art. 13º Quanto à utilização de equipamentos de informática particular, o funcionário deverá comunicar a equipe de informática para cadastrar login de acesso aos recursos da rede.

TÍTULO VI

DAS PROIBIÇÕES

Art. 14º Não é permitido utilizar, sem a autorização do setor de informática, equipamentos de rede (switches, pontos de acesso, etc.) com a finalidade de ampliar o número de pontos de acesso disponíveis no ambiente de trabalho ou de ensino.

Art. 15º Não será permitida a utilização de dados, aplicativos ou serviços que sobrecarreguem a rede de computadores.

Art. 16º Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso de recursos computacionais da rede do Instituto.

Art. 17º Não serão permitidas na rede do IF SERTÃO-PE a obtenção e propagação intencional de vírus worms, cavalos de tróia ou afins.

Art. 18º A instalação de jogos ou qualquer tipo de software/aplicativo que não for relacionado com trabalho serão proibidos.

Art. 19º É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pela Coordenação de Informática, através de solicitação via helpdesk.

Art. 20º Não é permitida a abertura de computadores para qualquer tipo de reparo, caso seja necessário, deverá ser feito pela equipe de informática.

TÍTULO VII

DAS PENALIDADES

Art. 21º O uso indevido dos recursos de TI do IF SERTÃO-PE será tratado como infração.

§ 1º Quando se tratar de servidor, o mesmo será notificado do descumprimento das normas estabelecidas.

§ 2º Persistindo a infração da norma, o servidor será novamente notificado, e será encaminhada cópia da notificação para sua chefia imediata ou para o Diretor do Campus ou, quando se tratar de servidor lotado na Reitoria, a notificação será encaminhada ao Pró-Reitor para abertura de processo disciplinar.

§ 3º Quando a violação das normas acontecer por parte de alunos, terceirizados ou estagiários, a notificação será encaminhada à Diretoria de Ensino ou ao Setor responsável para que sejam tomadas as providências.

§ 4º O usuário que cometer infração poderá responder processo disciplinar.

TÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 22º Esta regulamentação entra em vigor na data de sua publicação.

Art. 23º Os casos omissos serão dirimidos pelo Comitê Gestor de Tecnologia da Informação.

CAPITULO V

Regulamenta estabelece regras e diretrizes para os subdomínios, sítios e serviços eletrônicos na internet.

TÍTULO I

DO OBJETIVO

Art. 1º A gestão dos domínios, subdomínios, sítios e serviços eletrônicos na internet do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IF Sertão-PE) regem-se por esta Resolução (normativa):

TÍTULO II

DEFINIÇÕES

Art. 2 º Para fins desta Resolução, considera-se:

I – Domínio: nome atribuído a um determinado endereço no Sistema de Nomes de domínios (DNS) registrado diretamente sob um dos domínios de Primeiro Nível (DPN) definidos pelo Comitê Gestor da Internet no Brasil (CGI.br);

II – **Subdomínio:** nome vinculado a um domínio obedecendo a hierarquia a qual está vinculado, atribuído a um determinado endereço no Sistema de Nomes de domínios (DNS) registrado diretamente sob um domínio de Terceiro Nível (ifsertao-pe.edu.br) definidos pelo Comitê Gestor de Segurança da Informação (CGSI) do IF Sertão-PE;

III – **Página**: conteúdo acessado por intermédio de um Localizador de Recursos Unificado (URL-*Uniform Resource Locator*) disponibilizado na internet;

IV – **Sítio**: conjunto de páginas que disponibiliza informações e/ou serviços sob a responsabilidade de um Gestor de Sítio, podendo ser classificados como portais temáticos, promocionais, institucionais, entre outros;

V – **Serviço Eletrônico:** serviços prestados à sociedade ou à própria Administração por meio eletrônico e de forma automática com o objetivo equivalente àquele disponibilizado presencialmente.

VI – **Unidade Responsável:** departamento do IF Sertão-PE à qual pertence um domínio ou Subdomínio, Sítio ou Serviço Eletrônico;

VII – **Responsável pelo domínio e/ou subdomínio:** servidor público federal responsável pela área à qual um determinado domínio e/ou subdomínio está vinculado;

VIII – **Gestor de Sítio:** servidor público federal designado por um Responsável por domínio/subdomínio para responder por um Sítio;

TÍTULO III

DIRETRIZES PARA CRIAÇÃO DOS SUBDOMÍNIOS

Art. 3º Os domínios e subdomínios deverão seguir os seguintes padrões:

§ 1º Serão utilizados para os subdomínios de quarto nível (ifsertao-pe.edu.br):

I – Subdomínios que apresentem uso geral a todo o IF Sertão-PE utilizarão o nome simples que identifique o sítio, seguido de (ifsertao-pe.edu.br).

Ex.:

a. www.ifsertao-pe.edu.br -> Portal Institucional

b. sigaadm.ifsertao-pe.edu.br -> Sistema de Administração

c. concurso.ifsertao-pe.edu.br -> Sistema de Concursos

§ 2º Serão utilizados para os subdomínios de quinto nível (CAMPUS. ifsertao-pe.edu.br):

II – Para todos os Campi do IF Sertão-PE será adotado uma nomenclatura de identificação:

Ex.:

a. reitoria.ifsertao-pe.edu.br -> Reitoria
b. petrolina.ifsertao-pe.edu.br -> Campus Petrolina
c. zonarural.ifsertao-pe.edu.br -> Campus Petrolina Zona Rural
d. salgueiro.ifsertao-pe.edu.br -> Campus Salgueiro
e. ouricuri.ifsertao-pe.edu.br -> Campus Ouricuri
f. floresta.ifsertao-pe.edu.br -> Campus Floresta
g. santamaria.ifsertao-pe.edu.br -> Campus Santa Maria da Boa Vista
h. serratalhada.ifsertao-pe.edu.br -> Campus Serra Talhada

III – Subdomínios que apresentem uso local, apenas naquele Campus do IF Sertão-PE, utilizarão o nome simples que identifique o sítio, seguido de (CAMPUS.ifsertao-pe.edu.br).
Ex.:

a. helpdesk.reitoria.ifsertao-pe.edu.br -> Sistema de Helpdesk Reitoria
b. helpdesk.petrolina.ifsertao-pe.edu.br -> Sistema de Helpdesk Campus Petrolina
c. sage.petrolina.ifsertao-pe.edu.br -> Sistema Acadêmico Petrolina
d. sage.salgueiro.ifsertao-pe.edu.br -> Sistema Acadêmico Salgueiro
e. cti.petrolina.ifsertao-pe.edu.br -> Coord. de TI Petrolina
f. cti.ouricuri.ifsertao-pe.edu.br -> Coord. de TI Ouricuri
g. coinfo.ouricuri.ifsertao-pe.edu.br -> Coord. do Curso de Informática Ouricuri

Parágrafo Único: se o subdomínio não for de uso geral do IF Sertão-PE, este deverá ser vinculado ao subdomínio vinculado a um dos campi, sendo obrigatoriamente registrado com o nome simples seguido de (CAMPUS. ifsertao-pe.edu.br). O nome simples deve fazer referência ao projeto ou unidade responsável.

Art. 4º Poderão solicitar a disponibilização de um subdomínio:

§ 1º Todos os servidores públicos que possuam projetos no IF Sertão-PE aprovados pelo gestor máximo do campus ou reitoria.

§ 2º Responsáveis por:

I – Reitoria e Pró Reitorias

II – Diretorias;

III – Secretarias;

IV – Coordenações.

Art. 5º A solicitação deverá ocorrer formalmente através de documento oficial, devendo ser anexado ao mesmo o projeto com justificativas de criação do subdomínio.

Art. 6º A criação do subdomínio está condicionada a aprovação por parte do gestor máximo do campus ou reitoria.

Art. 7º A criação do subdomínio deverá ser realizada pela Diretoria de Gestão de TI na Reitoria e as Coordenações de TI dos Campi.

Art. 8º O subdomínio ficará disponível durante a vigência do projeto ou por período informado pelo solicitante.

Parágrafo Único: a qualquer momento o subdomínio poderá ser suspenso ou excluído mediante solicitação do dirigente máximo do Campus, Reitoria ou pelo próprio solicitante.

Art. 9º A criação do subdomínio não garante a disponibilidade de espaço de armazenamento nos servidores da Instituição para disponibilização de sítios.

TÍTULO IV

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 10º Compete ao Responsável pelo Domínio:

§ 1º subdividir o domínio em subdomínios de acordo com o interesse Institucional;

§ 2º garantir a disponibilidade e conformidade do domínio de acordo com esta normativa;

Art. 11º Compete ao solicitante do subdomínio:

§ 1º formalizar a solicitação por meio de documento oficial;

§ 2º responder subsidiariamente pelo conteúdo publicado nos Sítios e nos Serviços Eletrônicos sob sua responsabilidade sendo, portanto, o gestor do sítio;

§ 3º responder pela indisponibilidade de conteúdo do Sítio sem sua devida extinção;

§ 4º responder pelas falhas de segurança contido no sítio ou serviço eletrônico.

Art. 12º Compete à Unidade Responsável:

§ 1º designar o responsável pelo domínio e/ou subdomínio ou assumir suas funções e responsabilidades;

§ 2º registrar as informações relativas ao Domínio na DGTI ou CTI;

CAPITULO VI

Regulamenta a Política de Backup e Restauração de Dados

TÍTULO I

DO OBJETIVO

Art. 1º Esta norma estabelece a política de cópias de segurança (backup) e restauração de dados corporativos armazenados no parque tecnológico do IF SERTÃO-PE.

TÍTULO II

DO CAMPO DE APLICAÇÃO

Art. 2º Abrange os dados corporativos existentes nos servidores de rede.

Art. 3º As diretrizes estabelecidas no presente documento deverão ser aplicadas em todos os *Campi* que compõem o IF SERTÃO-PE, bem como na Reitoria.

TÍTULO III

DAS DEFINIÇÕES

Art. 4º Para os fins desta Instrução Normativa devem ser adotadas as seguintes definições:

I. **Backup:** cópia de dados de um dispositivo de armazenamento para outro, com o objetivo de recuperá-lo em caso de perda dos dados originais.
II. **Restauração:** processo de restauração de dados armazenados em subsistemas de discos e/ou biblioteca de fitas.
III. **Retenção:** período em que os dados ficarão retidos, guardados e/ou armazenados.
IV. **GFS (Grandfather-father-son)**: O método básico que consiste em criar três conjuntos de backup, sendo um diário, um semanal e outro mensal. Os backups diários (**son**) ou "filhos" são rotacionados a cada dia com um semanal (ou pai- **father**) a cada semana.

V. O backup semanal é rotacionado, em bases semanais, com um mensal ("ou avô"- **Grandfather**). Ocasionalmente, um volume pode ser removido do esquema para estabelecer um marco (milestone), ou para fins de Disaster Recovery.

VI. Backup full (backup completo): é a cópia de segurança completa dos arquivos especificados na estratégia de backup;

VII. Backup Diferencial / Incremental: é a cópia somente de arquivos novos ou modificados desde a última execução do backup;

TÍTULO IV

ORIENTAÇÕES GERAIS

Art. 5º Cabe aos administradores da rede, analistas de TI, técnicos de TI e gestores da instituição:

§ 1º Definir uma política de backup e restauração dos dados corporativos;

§ 2º Planejar, executar, monitorar e documentar as rotinas de backup;

§ 3º Restaurar quando necessário backup dos dados corporativos;

§ 4º Comunicar eventuais erros apresentados durante a execução da rotina de backup aos administradores responsáveis;

§ 5º Manter o storage de backup corretamente armazenado;

§ 6º Executar o procedimento automático ou manual de destruição das mídias de armazenamentos inservíveis;

§ 7º Solicitar suporte de terceiros em caso de falha nos dispositivos de armazenamento;

§ 8º Categorizar os dados baseando-se na prioridade de recuperação, delimitando o tempo de retenção;

§ 9º Homologar a política de backup nas unidades organizacionais;

§ 10º Prover os recursos necessários para implantar a política de backup;

§ 11º Planejar e executar a realização de testes periódicos de restauração dos backups.

§ 12º A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

§ 13º As mídias (ou dispositivos de armazenamento) deverão ser armazenados em locais seguros, de preferência em localidade diversa da origem dos dados (backup off-site).

§ 14º As solicitações de restauração de arquivos deverão ser abertas formalmente através de ferramentas de abertura de chamados (Helpdesk) e deverão conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso.

§ 15º O proprietário dos dados deverá ter ciência dos tempos de retenção aqui estabelecidos para cada tipo de informação;

§ 16º Os administradores/operadores de backup deverão zelar pelo cumprimento das diretrizes aqui estabelecidas.

TÍTULO V

NORMA PARA BACKUP DOS DADOS NAS ESTAÇÕES DE TRABALHO

Art. 6º O backup dos arquivos pessoais existentes nas estações de trabalho é de inteira responsabilidade dos usuários, que deverão fazê-lo em mídia própria;

Art. 7º Os dados corporativos criados ou mantidos pelos usuários deverão ser armazenados em local próprio indicado pelo departamento de TI do respectivo campus;

Art. 8º É de inteira responsabilidade dos usuários armazenar os dados corporativos em local apropriado conforme definido pelo departamento de TI;

Art. 9º É de responsabilidade dos usuários a execução periódica de cópias de segurança dos dados corporativos existentes em sua estação de trabalho, em mídia independente, assim como seu armazenamento nas dependências de seu respectivo departamento;

Art. 10º O departamento de TI não se responsabiliza pela integridade dos backups feitos pelos usuários em qualquer mídia de armazenamento;

Art. 11º O departamento de TI não se responsabiliza pela perda dos dados corporativos armazenados nas estações de trabalho ou em quaisquer mídias de armazenamento não indicadas pelo departamento.

TÍTULO VI

NORMAS PARA BACKUP DOS DADOS CORPORATIVOS

Art. 12º A estratégia de backup deverá conter, no mínimo, as seguintes informações:

I. A frequência e esquema de realização do backup;

II. O que deve ser copiado, ou seja, o escopo do backup;

III. O método de acesso aos dados;

IV. O local de armazenamento das cópias e as medidas de proteção dessas cópias;

V. Os tipos de cópia (Completa, Diferencial ou incremental) de segurança a serem executadas;

VI. A rotina de verificação de integridade (sucesso) do backup.

VII. Abrangência do backup:

a- Servidor Web;

b- Servidor de Banco de Dados;

c- Serviços de monitoramento;

d- Sistemas operacionais;

e- Servidores de Arquivos;

f- Máquinas Virtuais (imagem);

g- Servidores de E-mail;

h- Servidor Wifi e Controladora;

i- Firewalls

j- Servidores de CFTV;

k- Servidores de rede de computadores;

VIII. Os Itens excluídos do backup:

a- Quaisquer dados ou informações cujo backup não seja de responsabilidade da TI.

IX. Do esquema de realização do backup:

a- Será adotado o esquema de rotação de mídias de armazenamento GFS (Grandfather-father-son), exceto se especificada necessidade especial;

b- O método básico consiste em criar três conjuntos de backup, sendo um diário, um semanal e outro mensal. Os backups diários ou "filhos" são rotacionados a cada dia com um semanal (ou pai) a cada semana. O backup semanal é rotacionado, em bases semanais, com um mensal ("ou avô").

c- O backup é realizado na modalidade recuperação de desastre, que se refere à restauração dos dados em casos de inundação, terremoto, incêndio, dados e informações perdidas ou corrompidas.

TÍTULO VII

TESTE DE RECUPERAÇÃO DE DADOS

Art. 12º - Os testes serão realizados mensalmente e deverão obedecer aos seguintes parâmetros:

I - Deverá ser restaurado pelo menos um backup de cada fonte;

II - A realização dos testes e o seu resultado deverão ser registrados em documento próprio;

Parágrafo único - Caso ocorra falha na restauração, o servidor responsável deverá informar expressamente a Gerência para que tome as medidas necessárias à correção do problema.

TÍTULO VII

RECUPERAÇÃO DE DADOS

Art. 13º A recuperação de dados será realizada mediante solicitação via Helpdesk que deverá conter, no mínimo, os seguintes requisitos:

I - Sempre que possível, deverá ser informado:

a) O nome do arquivo ou da pasta;

b) o nome do servidor de rede em que o arquivo ou a pasta estavam armazenados;

c) o caminho de rede onde o arquivo ou a pasta estavam armazenados.

§1º - Em todos os casos deverá ser informada a data estimada da qual se deseja restaurar o backup.

§2º - O prazo para restauração do backup é de 72 (setenta e duas) horas corridas, podendo ser expandido quando a diferença entre a data da solicitação e a data estimada para restauração for superior a 6 (seis) meses.

CAPITULO VII

Regulamenta a utilização dos laboratórios de Informática

TÍTULO I

DO OBJETIVO

Art.1º - O presente documento contém as normas que regem e orientam as condições de utilização dos Laboratórios de Informática do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano

TÍTULO II

DO CAMPO DE APLICAÇÃO

Art.2º - Ficam sujeitos a este regulamento todos os usuários dos Laboratórios de Informática. **Parágrafo Único -** Todo usuário deverá cumprir as normas aqui contidas, favorecendo a coletividade e o aproveitamento máximo dos laboratórios para fins educacionais.

Art.3º - O Departamento de Ensino é responsável por elaborar, planejar e enviar as demandas contendo os softwares e ferramentas necessárias para as aulas do semestre subsequente até o final do semestre anterior. Exceções deverão ser solicitadas com antecedência de 5(cinco) dias úteis e sua viabilidade será julgada pelo setor responsável.

Parágrafo Único – Caso as demandas de softwares e ferramentas estejam em decurso de prazo, prevalecerá a demanda anterior.

Art.4º - Nas aulas, será de responsabilidade do professor da disciplina orientar os trabalhos e zelar pela ordem e correta utilização dos equipamentos. E, ao término dos trabalhos, o professor responsável deverá solicitar aos alunos que reorganizem as cadeiras em seus devidos lugares, desliguem os equipamentos corretamente, retornando-os à posição de origem, e que mantenham o ambiente limpo.

TÍTULO III

ORIENTAÇÕES GERAIS

Art.5º - Por questões legais referentes a lei vigente de Direitos Autorais, não é permitida a gravação, reprodução ou a utilização de quaisquer softwares sem a devida licença de uso.

Art.6º - É proibida a instalação ou remoção de softwares que não sejam devidamente autorizadas pelo técnico responsável do laboratório ou pelo Setor de tecnologia da informação.

Art.7º - É proibida a abertura de computadores sem a devida autorização do técnico responsável do laboratório ou pelo Setor de tecnologia da informação. Salvo os computadores específicos para as aulas práticas de manutenção com acompanhamento do professor.

Parágrafo Único - Caso seja necessário o reparo, este deverá ser feito pelo responsável técnico do laboratório ou pelo Setor de tecnologia da informação.

Art.8º - Qualquer problema nos equipamentos deve ser reportado ao técnico do laboratório ou ao Setor de tecnologia da informação, via chamado por Helpdesk, para que este seja solucionado.

Art.9º - Nenhum equipamento pode ser conectado à rede sem autorização prévia do Setor de tecnologia da informação.

Art.10º - Será feita, ao final de cada semestre letivo, a limpeza dos arquivos armazenados nos computadores dos laboratórios para que não haja acúmulo desnecessário de informações.

Parágrafo único – Recomenda-se que os usuários façam cópia de segurança dos seus arquivos que são utilizados nos laboratórios.

Art.11º - Os usuários dos laboratórios comprometem-se a utilizar os recursos exclusivamente para atividades de ensino, pesquisa e extensão.

Art.12º- Os usuários só terão acesso aos laboratórios nos horários previstos para aulas ou em casos excepcionais com autorização do Departamento de Ensino.

Art.13º - Não havendo agendamento dos laboratórios para o referido horário, e havendo disponibilidade, o mesmo poderá ser utilizado para outras atividades, como curso de extensão, aulas de reforço, monitoria de curso e outras práticas habilitadas pelas Coordenações do campus e autorizadas pelo Departamento de Ensino.

Art.14º - É proibido nos Laboratórios:

a) Remover ou Danificar equipamentos e periféricos (mouse, teclado, monitor de vídeo, entre outros.);

b) Gravar CDs e DVDs, salvo com consentimento do professor, técnico responsável ou Setor de tecnologia da informação;

c) Trazer ou retirar mesas e cadeiras sem prévia autorização do Departamento de Ensino ou do Patrimônio;

d) Desenvolver, disseminar ou utilizar programas que tenham objetivo de obter senhas, informações pessoais de outros usuários ou acessar informações restritas;

e) Utilização de jogos para fins não educacionais;

f) Acessar páginas ou utilizar software com conteúdo pornográfico;

g) Fumar e/ou consumir qualquer tipo de alimento ou bebidas;

h) Utilizar os equipamentos para fins pessoais ou qualquer outro tipo de atividade incompatível com as tarefas acadêmicas;

Parágrafo único – O Setor de tecnologia da informação não se responsabilizará por equipamentos de uso pessoal.

Art.15º - Os usuários que praticarem qualquer ação em desacordo com esse normativo ou outra que resulte em danos aos laboratórios estarão sujeitos às sanções disciplinares previstas no Regimento do Campus.

Art.16º - Caso o usuário tenha dúvida a respeito de realizar alguma atividade, deve consultar o Departamento de Ensino ou Setor de tecnologia da informação.

Art.17º - Algumas recomendações que constituem boas práticas de utilização dos laboratórios:

a) Os computadores devem ser desligados no final da seção diária de trabalho pelos próprios usuários;

b) Arquivos gravados, pelo usuário, em discos rígidos devem ser copiados para seu dispositivo de armazenamento pessoal ao terminar a sessão diária de uso;

c) Problemas e ocorrências estranhas observadas com o equipamento devem ser reportados ao professor ou Setor de tecnologia da informação, conforme o caso;

d) As cadeiras devem ser reorganizadas após o uso dos laboratórios.

Art.18º- Os alunos, no ato da matrícula, assinarão um termo de compromisso, comprometendo-se a seguir as Políticas de Segurança e dando ciências das normas estabelecidas.

Parágrafo Único - O termo de compromisso é utilizado para que os alunos se empenhem formalmente em seguir as Políticas de Segurança, tomando ciência das punições impostas ao seu não cumprimento.

Art.19º - Os casos omissos nesta Instrução Normativa serão resolvidos pelo Departamento de Ensino e/ou Setor de tecnologia da informação, consultando, se necessário, outros setores da instituição, assim como a Direção Geral do Campus.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

DO SERTÃO PERNAMBUCANO

REGIMENTO INTERNO DO

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - CGSI

Petrolina/PE

2015

TÍTULO I
DA FINALIDADE

Art. 1º - O presente Regimento tem por finalidade estabelecer os aspectos de organização e de funcionamento do Comitê Gestor de Segurança da Informação – CGSI junto ao Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – IFSERTÃO-PE.

TÍTULO II
DA COMISSÃO

Art. 2º. O Comitê Gestor de Segurança da Informação, de – CGSI, de caráter propositivo, tem como finalidade:

I – Criar políticas e diretrizes para a segurança da informação e comunicação na IFSERTÃO-PE;

II – Implementar as políticas de segurança da informação e comunicação na IFSERTÃO-PE após aprovação;

III – Divulgar as políticas de segurança da informação e comunicação na IFSERTÃO-PE para todos os servidores e comunidade acadêmica.

SEÇÃO I
DA COMPOSIÇÃO

Art. 3º. O Comitê Gestor de Segurança da Informação será composto por:

I - Diretor da Diretoria de Gestão de Tecnologia da Informação - DGTI;

II. - Representantes de TI de cada Campus;

III. - Representantes da área de negócio.

Parágrafo único – Os representantes da área de negócio serão indicados no campus pelo Diretor Geral e, na Reitoria, pelo Reitor.

SEÇÃO II
DA PRESIDÊNCIA

Art. 4º - A presidência da CGSI será exercida pelo candidato eleito e na ausência um servidor será indicado pelo presidente para exercer a função de suplente da presidência.

I - O mandato será de 2 (dois) anos.

II. -. O novo presidente será escolhido, paritariamente, dentre os membros para um mandato de dois anos.

SEÇÃO III
DAS ATRIBUIÇÕES

DO PRESIDENTE

Art. 5º – São atribuições do Presidente:

I. Coordenar o Comitê de Segurança da Informação e Comunicações;

II. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;

III. Representar o Comitê nos atos que se fizerem necessários;

IV. Definir datas e pautas para convocações, convocar, abrir, presidir, suspender, prorrogar e encerrar as reuniões e resolver questões de ordem;

V. Solicitar esclarecimentos que lhe forem úteis à melhor apreciação dos assuntos em pauta;

VI. Submeter ao debate e à votação as matérias a serem deliberadas, apurando os votos e proclamando os resultados;

VII. Decidir em caso de empate, utilizando o voto de qualidade;

VIII. Autorizar a presença nas reuniões de pessoas que possam contribuir para os trabalhos do Comitê;

IX. Indicar membros para realizações de estudos, levantamentos, investigações e emissão de pareceres necessários à consecução da finalidade do Comitê Gestor de Segurança da Informação, bem como relatores das matérias a serem apreciadas;

X. Designar servidores responsáveis pelos trabalhos de apoio operacional e administrativo às reuniões do Comitê.

DOS DEMAIS MEMBROS

Art. 6º – São atribuições dos demais membros;

I. Comparecer às reuniões ordinárias e extraordinárias do Comitê Gestor de Segurança da Informação;

II. Analisar, discutir e votar as matérias em discussão;

III. Realizar estudos e pesquisas, apresentar proposições, apreciar, emitir pareceres e relatar as matérias que lhe forem submetidas;

IV. Sugerir normas e procedimentos necessários ao bom funcionamento das atividades do Comitê Gestor de Segurança da Informação;

V. Propor e requerer esclarecimentos que lhes forem úteis à melhor apreciação da matéria em pauta;

VI. Indicar técnicos ou representantes de unidades administrativas, de outros órgãos ou entidades, que possam contribuir para esclarecimentos e subsídios sobre matérias constantes da pauta ou desenvolvimento das atividades do Comitê Gestor de Segurança da Informação;

VII. Fazer cumprir, em suas respectivas unidades, as resoluções emanadas e aprovadas pelo Comitê;

VIII. Propor a inclusão de matérias na pauta das reuniões;

IX. Comunicar ao Presidente, com antecedência mínima de 48 (quarenta e oito) horas, a impossibilidade do seu comparecimento à reunião.

SEÇÃO IV
DAS REUNIÕES

Art. 7º - A CGSI reunir-se-á, ordinariamente, a cada semestre e extraordinariamente, quando convocado pelo Presidente ou por pelo menos 2/3 (dois terços) dos representantes com direito a voto das unidades.

§1º - Terão direito a voz todos os membros da CGSI;

§2º - Terão direito a voto os representantes, de cada unidade;

§3º - O Presidente terá direito a voto somente em caso de empate na votação;

§4º - As reuniões ordinárias da CGSI serão agendadas com, no mínimo, 1 Mês de antecedência presencialmente, caso seja virtualmente, 1 semana de antecedência.

Art. 8º - Poderão ser agendadas reuniões em conjunto com outros comitês vinculados às atividades da CGSI, para assessoramento em assuntos específicos.

Art. 9 - Para o desenvolvimento das atividades da CGSI poderão ser organizados Grupos de Trabalho (GTs), de modo a operacionalizar as demandas específicas.

SEÇÃO V
DAS ATRIBUIÇÕES DO COMITÊ

Art. 10 – São atribuições da CGSI:

XI. Assessorar na implementação das ações de segurança da informação e comunicações no IFSERTÃO-PE;

XII. Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;

XIII. Sugerir ações visando ao alinhamento do plano de desenvolvimento de tecnologia da informação com o planejamento estratégico do Instituto como um todo;

XIV. Apresentar sugestões e críticas com a finalidade de alinhar as áreas de negócio e todas as áreas envolvidas na disponibilização da infraestrutura tecnológica dos órgãos incluindo as áreas de informática, de logística, de contratação, entre outras, no âmbito da Segurança da Informação;

XV. Elaborar a Política de Segurança da Informação e Comunicações - POSIC e sua respectiva atualização;

XVI. Apreciar e emitir parecer sobre os relatórios das atividades desenvolvidas;

TÍTULO III
DAS DISPOSIÇÕES GERAIS

Art. 11 – Este regimento poderá ser revisto por solicitação de no mínimo 2/3 (dois terços) do quantitativo total dos membros da CGSI.

Art. 12 – Este Regimento entrará em vigor após a sua aprovação pelo Conselho Superior do IFSERTÃO-PE.