Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia do Piauí
IFPI
Av. Jânio Quadros, 330, Santa Isabel, TERESINA / PI, CEP 64053-390
Fone: (86) 3131-1443 Site: www.ifpi.edu.br

RESOLUÇÃO NORMATIVA CONSUP/OSUPCOL/REI/IFPI N° 232, de 19 de dezembro de 2024.

Atualiza a Política de Segurança da Informação, o uso do Correio Eletrônico Institucional e as Normas de Segurança para criação de senhas, no Instituto Federal de Educação, Ciência e Tecnologia do Piauí (IFPI), e dá outras providências.

O Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, no uso de suas atribuições conferidas no Estatuto deste Instituto Federal, aprovado pela Resolução Normativa nº 59, de 20 de agosto de 2021, publicada no Diário Oficial da União de 23 de agosto de 2021, considerando o processo nº 23172.003821/2023-26, deliberação em reunião do dia 18 de dezembro de 2024, e ainda:

a 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 (APF) direta e indireta;
a Instrução Normativa GSI nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal direta e indireta, e dá outras providências;
a Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, capítulo IV;
a Norma Complementar (NC) nº 02/IN01/DSIC/GSIPR – Metodologia de Gestão de Segurança da Informação e Comunicações;
a NC nº 03/IN01/DSIC/GSIPR – Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações na Administração Pública Federal (APF);
a NC nº 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações na APF;
a NC nº 05/IN01/DSIC/GSIPR (revisada em 2013) – Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais na APF;
a Instrução Normativa 01/GSI/PR, Art.12, Inciso IV, alínea g, h;
a NC nº 06/IN01/DSIC/GSIPR – Gestão de Continuidade de Negócios na APF;
a NC nº 07/IN01/DSIC/GSIPR (revisada em 2014) – Implementação de Controles de Acesso na APF;
a NC nº 08/IN01/DSIC/GSIPR – Gerenciamento de Incidentes em Redes Computacionais na APF;
a NC nº 09/IN01/DSIC/GSIPR (revisada em 2014) – Uso de Recursos Criptográficos na APF;
a NC nº 10/IN01/DSIC/GSIPR – Inventário e Mapeamento de Ativos de Informação na APF;
a NC nº 11/IN01/DSIC/GSIPR – Avaliação de conformidade na APF;
a NC nº 12/IN01/DSIC/GSIPR – Dispositivos Móveis na APF;
a NC nº 13/IN01/DSIC/GSIPR – Gestão de Mudanças na APF;
a NC nº 14/IN01/DSIC/GSIPR – Tecnologias de Computação em Nuvem na APF;
a NC nº 15/IN01/DSIC/GSIPR – Uso de Redes Sociais na APF;

a NC nº 16/IN01/DSIC/GSIPR – Desenvolvimento e Obtenção de Software Seguro na APF;
a NC nº 17/IN01/DSIC/GSIPR – Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações na APF;
a NC nº 18/IN01/DSIC/GSIPR – Atividades de Ensino em Segurança da Informação e Comunicações na APF;a NC nº 19/IN01/DSIC/GSIPR – Padrões Mínimos de Segurança da Informação e Comunicações na APF;
a NC nº 20/IN01/DSIC/GSIPR – Instituição do Processo de Tratamento da Informação na APF;
a NC nº 21/IN01/DSIC/GSIPR – Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes na APF;
o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação e suas alterações no DECRETO Nº 10.641, DE 2 DE MARÇO DE 2021 ;
o Decreto nº 9.690, de 23 de janeiro de 2019, que altera o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação;
o Decreto nº 7.579/2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;
o Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER), Anexo, Item 2.3.4 e 2.3.5;
o Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), Anexo, art. 3º, Incisos I, II e V;
o Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI), Cap. I - Art. 2º, Incisos III e IV, Cap. II - Art. 3º, Incisos III, IV, VIII XI; e cap. VI - Seção IV – Art. 15;
o Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022 combinado com o Decreto nº 11.260, de 22 de novembro de 2022;
o Decreto nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD), Art. 2º, XXIII com as alterações do Decreto nº 11.226/2022;
o Decreto nº 11.529, de 16 de maio de 2023, que dispõe sobre o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal;
a 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;
a Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;
a Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados, cap. VII - Seção I – Art. 46, Seção II, Art. 50;
a Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI);
a ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos;
a ABNT NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão de Segurança da Informação;
a ABNT NBR ISO/IEC 27005:2011 – Tecnologia da Informação - técnicas de segurança - código de prática para a gestão de segurança da informação;
a Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da Informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos, A.12.3 - cópias de segurança;
a Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação, 12.3 Cópias de segurança;
a Aplicação de boas práticas em Tecnologia da Informação recomendada pela Corte de Contas da União (TCU) e assinaladas na edição dos Acórdãos 1603/2008 - Plenário, 71/2007 – Plenário, 1092/2007 - Plenário e 2023/2005 – Plenário;

o Acórdão do Tribunal de Contas da União nº 461/2004, de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;
o Acórdão 1.109/2021-TCU-Plenário;
o Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI, v4.1: DS11: Gerenciar Dados; v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06;
o Guia do Framework de Privacidade e Segurança da Informação, controle 11;
o Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI, Gestão da Segurança da Informação;
a Portaria Interministerial nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet e dá outras providências;
a Portaria GSI/PR nº 93, de 18 de outubro de 2021;
o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;
o Decreto 12.069, de 21 de junho de 2024 - Estratégia de Governo Digital 2024-2027;
o GSI 09/2023. OSIC (ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA) — Gestão de Acesso Privilegiado (Privileged Access Management – PAM) – parte 2 de 2. Disponível em: https://www.gov.br/gsi/pt-br/ssic/osic/OSIC%2009.23;
a ISO/IEC FDIS 29151:2016(E). Information technology — Security techniques — Code of practice for personally identifiable information protection Itens 9 – 9.2.2 e 9.2.3 (Página 11);
a ABNT NBR ISO/IEC 27701: 2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e Diretrizes Itens 6 – 6.6.2 (Página 16);
a Account and Credential Management Policy Template for CIS Controls 5 and 6;
a Portaria GSI/PR nº 93, de 18 de outubro de 2021;
a Instrução Normativa Nº 04/GSI/PR, de 26 de março de 2020 Capítulo II; e
o Guia do Framework de Privacidade e Segurança da Informação (PPSI).

RESOLVE:

Art. 1º Atualizar a Política de Segurança da Informação e Comunicação (POSIC), de uso do Correio Eletrônico Institucional e as Normas de Segurança para criação de senhas no IFPI.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A Política de Segurança da Informação e Comunicação (POSIC) tem como objetivo estabelecer diretrizes, critérios e procedimentos para proteger os ativos de informação e a gestão da Segurança da Informação (SI), tendo como complemento a política de uso do Correio Eletrônico Institucional e as normas de segurança para criação de senhas dentro da rede do IFPI.

Art. 3º As regras e metas estabelecidas nesta POSIC serão aplicadas em todos os níveis da instituição, sendo eles: estratégico, tático e operacional.

Parágrafo único. As diretrizes que irão balizar o uso dos ambientes, sistemas, recursos computacionais e redes informacionais em todos os campi e na Reitoria são aplicáveis à comunidade interna e à externa do IFPI.

Art. 4º A Diretoria de Tecnologia da Informação (DTI) fundamenta a POSIC, o uso do Correio Eletrônico Institucional e as Normas de Segurança para criação de senhas e

utilização de recursos computacionais, considerando um conjunto de decretos, instruções normativas e normas complementares.

CAPÍTULO II
DOS OBJETIVOS GERAIS E ESPECÍFICOS DA POSIC

Seção I
Dos Objetivos Gerais

Art. 5º A Diretoria de Tecnologia da Informação (DTI) do IFPI considera os objetivos gerais segundo o art. 4º do Decreto nº 9.637/2018, de 26 de dezembro de 2018.

Seção II
Dos Objetivos Específicos

Art. 6º São Objetivos Específicos da POSIC:

I - estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional no IFPI;

II - constituir, determinar ou reorganizar as funções e atribuições do grupo responsável pela Segurança da Informação no âmbito institucional; e

III - viabilizar a confecção de mecanismos de controle, além de promover a otimização dos recursos e investimentos em Tecnologia da Informação (TI).

Art. 7º A Política de uso do Correio Eletrônico Institucional do IFPI tem como objetivo estabelecer critérios gerais, atribuições e obrigações para uso de correio eletrônico no IFPI.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 8º São princípios da POSIC:

I - confidencialidade: somente pessoas devidamente autorizadas pela organização devem ter acesso à informação;

II - integridade: somente operações de alteração, supressão e adição autorizadas pela organização devem ser realizadas nas informações;

III - disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

IV - autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

V - criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição; e

VI - não-repúdio: garantia que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.

Parágrafo único. Toda informação produzida ou recebida pelos membros da comunidade interna ou externa do IFPI, como servidores docentes, técnico-administrativos, discentes, visitantes, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao IFPI. As exceções devem ser explicitadas e formalizadas entre as partes.

CAPÍTULO IV

DOS CONCEITOS E DEFINIÇÕES

Art. 9º Para efeitos da POSIC e das normas vinculadas a ela, define-se:

I - ação de evitar o risco: decisão de não se envolver ou agir de forma a se retirar de uma situação de risco (NBR ISO/IEC 27005, 2008);

II - aceitar/reter o risco: aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco (NBR ISO/IEC 27005, 2008);

II - ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ISO/IEC 27000, 2014);

IV - ativo: qualquer coisa que tenha valor para a organização (NBR ISO/IEC 27002, 2005);

V - insumos críticos de Tecnologia da Informação: abrange todos os ativos de Tecnologia da Informação, indispensáveis às atividades alvo do IFPI, conforme devem estabelecer as ações estratégicas da instituição;

VI - fonte de conhecimento: dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados no âmbito do IFPI. Exemplos desses ativos: base de dados, arquivos, acervo bibliográfico, registros acadêmicos, contratos, acordos, documentação de sistema, informações sobre pesquisa e extensão, manuais de usuário, material de treinamento, projetos técnicos de infraestrutura elétrica e de construção civil, procedimentos e planos institucionais, processos de trabalho e outros;

VII - insumos de Tecnologia da Informação: contempla os ativos físicos e de software, os quais permitem o armazenamento, a transmissão e o processamento das informações. Dentre esses, podem-se destacar os aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. Os insumos físicos compreendem o pátio de equipamentos computacionais do IFPI, o qual é formado por servidores de rede, computadores fixos e móveis, além dos dispositivos de intercomunicação (roteadores, switchs, pontos de acesso e outros);

VIII - responsável legal: reitor, pró-reitores, diretores ou coordenadores em geral, responsáveis pela(s) informação(ões) que esteja(m) atrelada(s) ao exercício dos cargos e funções supracitadas, bem como aos seus subordinados;

IX - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário (ISO/IEC 27000, 2014);

X - contas de acesso: formadas por uma identificação única, concedida de forma pessoal e intransferível a uma pessoa e por um método de autenticação. Esse par de informações habilita o seu dono a acessar equipamentos, sistemas e aplicações específicas, áreas restritas, de acordo com o perfil pré-definido;

XI - nível da informação: identificação do nível de proteção requerido pela mesma, atribuído pelo responsável legal;

XII - mitigar/reduzir o risco: efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco (NBR ISO/IEC 27005, 2008);

XIII - política: intenções e diretrizes da organização, formalmente expressas pela direção da Instituição (ISO/IEC 27000, 2014);

XIV - risco: efeito da incerteza sobre os objetivos de segurança da informação; é

associado com o potencial de que as ameaças irão explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização (ISO/IEC 27000, 2014);

XV - segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade das informações (ISO/IEC 27000, 2014);

XVI - vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças (ISO/IEC 27000, 2014);

XVII - servidor(a): pessoa legalmente investida em cargo público;

XVIII - auditoria: procedimentos para verificar se os sistemas e aplicativos são apropriados, eficientes e controlados adequadamente para garantir que a entrada, o processamento e a saída de dados são válidos, confiáveis, oportunos e seguros, em todos os níveis de atividade de um sistema;

XIX - ativo de Informação: corresponde a um recurso corporativo, como processamento de informações, armazenamento, sistemas de informações, procedimentos de suporte;

XX - backup ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

XXI - log: registro de eventos relevantes em um dispositivo ou sistema computacional;

XXII - padrão de Formação de Endereços de Correio Eletrônico: manual para definir o padrão a ser adotado na formação e criação de endereços de correio eletrônico (e-mails) dos servidores, empregados, ocupantes de funções e contratados de órgãos da Administração Pública Federal direta, autárquica e fundacional, e os das demais organizações públicas que se utilizarem do serviço de mensagens do Governo Federal; e

XXIV - Framework SGD: guia operacional elaborado pela Secretaria de Governo Digital (SGD), da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia para fomentar a adequação à proteção dos dados pessoais.

Art. 10. Para a política de uso do Correio Eletrônico Institucional e das vinculadas a ela, define-se:

I - domínio organizacional: nome que identifica, de forma única, no âmbito da Internet, uma organização. Exemplo: ifpi.edu.br, cefetpi.br;

II - domínio de rede: nome que identifica uma rede local ou distribuída geograficamente. Tem apenas significado local na organização;

III - identificador único: é o mecanismo que identifica, de forma única, uma pessoa física em um domínio de rede. Este identificador pode variar conforme a origem do usuário, a exemplo dos servidores do IFPI que utilizam seu identificador SIAPE e prestadores de serviços que utilizam o seu Cadastro de Pessoa Física (CPF);

IV - usuário: é a pessoa física com vínculo permanente ou temporário com o IFPI e que utiliza recursos e serviços de um domínio de rede;

V - unidade corporativa: instância administrativa do IFPI pertencente ao seu organograma;

VI - nome de usuário: conjunto de caracteres que identifica um usuário ou

unidade corporativa ("nome de usuário"@ifpi.edu.br);

VI - conta de usuário: recurso que permite a um usuário ter acesso aos serviços disponíveis em um domínio de rede. A existência da conta de usuário é imprescindível para que ele possa utilizar qualquer outro recurso ou serviço disponível na rede;

VII - conta de unidade corporativa: recurso que permite o armazenamento de mensagens de correio eletrônico;

VIII - serviço de correio eletrônico: recurso que permite ao usuário a troca de mensagens eletrônicas entre usuários de serviços de correio eletrônico. Um serviço de correio eletrônico está, necessariamente, vinculado à existência de uma conta de usuário;

IX - endereço de correio eletrônico: identificador de um usuário em um domínio organizacional para o serviço de correio eletrônico. Esse identificador é único para um dado domínio organizacional. O endereço de correio eletrônico é mandatório apenas para o usuário que utiliza o serviço de correio eletrônico. Uma conta de correio eletrônico poderá estar associada a mais de um endereço de correio eletrônico, atendido o critério da unicidade do identificador;

X - cota de armazenamento de correio eletrônico: quantidade de espaço de armazenamento disponibilizado na rede para conteúdo do serviço de correio eletrônico;

XI - custodiante da informação: qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

XII - eliminação: exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XIII - mídia: mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

XIV - infraestrutura crítica: instalações, serviços, bens e sistemas, virtuais ou físicos, que, se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

XV - Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TIC devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente; e

XVI - Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente.

Art. 11. Todos os usuários dos serviços de correio eletrônico do IFPI deverão estar inscritos no domínio “ifpi.edu.br”.

Art. 12. O domínio “ifpi.edu.br" será utilizado apenas para contas de correio eletrônico de cunho institucional.

CAPÍTULO V
DA COMPOSIÇÃO E COMPETÊNCIAS

Seção I
Da Composição

Art. 13. A Gestão de Segurança da Informação e Comunicação, no IFPI, é composta por:

I - Gestor de Segurança da Informação e Comunicação (GSIC);

II - Comitê de Segurança da Informação e Comunicação (CSIC); e

III - Equipe de Tratamento de Incidentes em Segurança da Informação (ETISI).

Seção II
Das Competências

Art. 14. Compete ao Comitê de Segurança da Informação e Comunicações:

I - assessorar na implementação das ações de segurança da informação e comunicações no órgão ou entidade da APF;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e

III - propor normas e procedimentos internos relativos à segurança da informação e comunicação, em conformidade com a legislação existente sobre o tema.

Art. 15. Compete ao Gestor de Segurança da Informação e Comunicação:

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 comunicação;

IV - coordenar o Comitê de Segurança da Informação e Comunicação e 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 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 comunicação; e

VII - propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

Art. 16. Compete ao Reitor, Pró-Reitores, Diretores, Chefes de Departamento e Coordenadores do IFPI:

I - viabilizar o acesso ao conjunto de documentos atualizados que compõem a POSIC aos seus subordinados;

II - adotar as diretrizes da POSIC nos processos de trabalho referentes a sua gestão; e

III - exigir o cumprimento da POSIC pelos servidores sob sua gestão.

Art. 17. Compete ao usuário (interno e externo):

I - conhecer e cumprir as diretrizes e normas desta POSIC;

II - responsabilizar-se por todo e qualquer acesso aos ativos de informação do IFPI, bem como pelos efeitos desse acesso, realizado por meio de seu código de identificação;

III - comunicar o mais breve possível os incidentes de segurança da informação, por ele conhecido, ao setor responsável; e

IV - colaborar com as investigações de incidentes, envolvendo direta ou indiretamente sua área.

Art. 18. O IFPI constituirá Equipe de Tratamento de Incidentes em Segurança da Informação (ETISI), e seu documento de constituição adotará as recomendações da Norma Complementar nº 05 /IN01/DSIC/GSI/PR, de 14 de agosto de 2009.

CAPÍTULO VI
DAS DIRETRIZES GERAIS E ESPECÍFICAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIC) E DE USO DO CORREIO ELETRÔNICO INSTITUCIONAL DO IFPI

Seção I
Das Diretrizes Gerais da POSIC

Art. 19. São diretrizes gerais da Política de Segurança da Informação e Comunicação do IFPI:

I - estar alinhada aos objetivos estratégicos, processos, requisitos legais e estrutura do IFPI, bem como ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);

II - estabelecer medidas e procedimentos para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações; e

III - observar as boas práticas e procedimentos de Segurança da Informação e Comunicação recomendados por órgãos e entidades responsáveis pelo estabelecimento de padrões.

Art. 20. É dever de todos os usuários da informação zelar pela Segurança da Informação e Comunicação.

Seção II
Das Diretrizes Específicas da POSIC

Art. 21. São diretrizes específicas da POSIC:

I - tratamento da informação;

II - tratamento de Incidentes de Rede;

III - política de backup;

IV - registros (logs) de Auditoria;

V - gestão de riscos;

VI - gestão de continuidade;

VII - auditoria e conformidade;

VIII - controle de acesso;

IX - acesso à Internet;

X - gestão de ativos de informação;

XI - segurança física e do ambiente;

XII - segurança em recursos humanos;

XII - gestão de operações e comunicações;

XIV - criptografia;

XV - desenvolvimento seguro de software; e

XVI - uso de e-mail;

Subseção I
Do Tratamento da Informação

Art. 22. As informações existentes no âmbito do IFPI apresentam diferentes níveis de confidencialidade e devem ser classificadas de acordo com a legislação vigente.

Parágrafo único. De acordo com o framework SGD, será nomeado um encarregado de dados para realizar essa classificação.

Art. 23. Normas complementares estabelecerão procedimentos que visem garantir a integridade, a confidencialidade e a disponibilidade das informações, incluindo procedimentos para a criação, manutenção e verificação dos ativos de informação e de suas cópias de segurança.

Subseção II
Do Tratamento de Incidentes de Rede

Art. 24. O IFPI deve manter equipe para tratamento e resposta a incidentes de segurança da informação, de modo que seja capaz de extrair informações e propor medidas que corrijam a falha que ocasionou o incidente.

Art. 25. É de responsabilidade da equipe de TI dos campi o acompanhamento e resolução dos incidentes de segurança notificados pelo CAIS/RNP.

Parágrafo único. A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) central na Reitoria, em colaboração com o Gestor de Segurança da Informação, desenvolverá um trabalho conjunto com as ETIRs dos campi, com o objetivo de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores conforme estabelecido na RESOLUÇÃO NORMATIVA CONSUP/OSUPCOL/REI/IFPI N° 189, de 12 de dezembro de 2023.

Subseção III
Da Política de Backup

Art. 26. É dever das equipes de TI locais (Reitoria e campi) implementar e automatizar a rotina de backup dos ativos de rede, garantindo assim a continuidade dos serviços do IFPI.

Art. 27. É de responsabilidade de cada usuário proceder com o backup de seus respectivos arquivos, estando as equipes de TI locais (Reitoria e campi) responsáveis apenas por prover os meios necessários para tal.

Parágrafo único. Recomenda-se o armazenamento apenas de arquivos institucionais. (Redação dada pela Lei nº 8.159, de 1991).

Art. 28. Os procedimentos de backup dos sistemas estruturantes serão

regulamentados pela política institucional implementada pela DTI. Os campi que possuírem sistemas anteriores à RESOLUÇÃO NORMATIVA CONSUP/OSUPCOL/REI/IFPI Nº 191, de 13 de dezembro de 2023, deverão desenvolver políticas locais em conformidade com o modelo disponibilizado pela Reitoria.

Art. 29. A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo Departamento de Tecnologia da Informação DTI e formalmente definidos como de necessária salvaguarda no Instituto Federal do Piauí, para se manter a continuidade do negócio.

§ 1º No sentido de assegurar sua missão, é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

§ 2º O documento apresenta a Política de Backup e Restauração de Dados Digitais, em que se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

§ 3º Esta política se aplica a todos os dados e servidores no âmbito do Instituto Federal do Piauí, que podem ser criadores e/ou usuários de tais dados, bem como a terceiros que acessam e usam no IFPI sistemas e equipamentos de TI ou que criam, processam e armazenam dados de propriedade do IFPI, incluindo dados fora do Instituto armazenados em um serviço de nuvem Pública ou Privada.

Art. 30. A Política de Backup e Restauração de Dados deve estar alinhada:

I - com a Política de Segurança da Informação do IFPI; e

II - com uma gestão de continuidade de negócios em nível organizacional.

§ 1º As rotinas de backup devem:

I - ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI;

II - utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada; e

III - possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

§ 2º O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto, distante do da sede da organização, para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

§ 3º A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

§ 4º Manter reserva de recursos físicos e lógicos de infraestrutura para realização de teste de restauração de backup.

§ 5º Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Art. 31. Os serviços de TI críticos da instituição devem ser formalmente elencados pelo CGTI do IFPI na referida política.

Art. 32. A salvaguarda dos dados em formato digital pertencentes a serviços de TI do IFPI, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

§ 1º Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).

§ 2º Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

§ 3º Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

§ 4º O Plano de Backup e a Política de Backup e Restauração dos ativos críticos do IFPI encontram-se resguardados pela DTI devido à criticidade dos dados e para promover a Segurança da Informação.

Subseção IV
Registros (Logs) de Auditoria

Art. 33. A coleta de logs de auditoria registra os eventos realizados pelos usuários nos ativos de TI. Os logs são gerados por diversas fontes, incluindo software de segurança, antivírus, firewalls e sistemas de prevenção e detecção de intrusão, sistemas operacionais em servidores, estações de trabalho e equipamentos de rede e aplicações.

§ 1º A geração de logs de auditoria de eventos realizados pelos usuários deve estar habilitada nos ativos de informação, seguindo as diretrizes desta política.

§ 2º Logs e registros de auditoria de ativos de informação devem ser coletados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

§ 3º Quando possível logs devem ser coletados em um ou mais repositórios centrais.

§ 4º Ativos de informação classificados como críticos devem ter logs de auditoria registrados conforme legislação pertinente.

§ 5º Quando possível, ativos de informação do IFPI devem gerar registros de logs de auditoria para eventos definidos. Esses eventos definidos incluem a identificação de eventos significativos relevantes para a segurança da informação que precisam ser auditados.

§ 6º Os ativos de TI considerados críticos para o IFPI devem ter registrados os eventos de:

I - tentativas de logon (do sistema ou domínio) bem-sucedidas e mal-sucedidas;

II - gerenciamento de contas de usuários;

III - acesso ao serviço de diretório;

IV - uso privilegiado;

V - acompanhamento de processos;

VI - sistema; e

VII - destruir arquivos de logs de auditoria.

§ 7º Ativos de informação em que os logs de auditoria contenham dados sensíveis devem ter registros de eventos que permitam ajudar em uma eventual investigação forense, como por exemplo: identificação inequívoca do usuário que acessou o recurso; natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc; data e hora do evento; e endereço IP, identificador do ativo de informação e outras informações que possam identificar a possível origem do evento.

§ 8º Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (Logs) em formato que permita a completa identificação dos fluxos de dados.

Art. 34. O IFPI, na medida do possível, deve centralizar a retenção de logs de auditoria de eventos realizados pelos usuários em seus ativos de informação com o objetivo de aperfeiçoar o gerenciamento destes logs.

§ 1º Ao definir o período de retenção de logs deve-se observar a definição legal de tempo de retenção/guarda/arquivamento de documentos e/ou dos dados tratados pelo IFPI.

§ 2º Os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável, quando possível.

§ 3º Quando houver necessidade de transferência de logs para armazenamento alternativo deve-se proteger a confidencialidade e integridade dos registros de auditoria.

§ 4º No caso de os logs armazenados contiverem dados pessoais, deve-se observar o previsto pela Lei Geral de Proteção aos Dados (LGPD), a fim de avaliar se os logs devem ser eliminados ou conservados após o término do tratamento dos dados pessoais.

§ 5º Registros de logs auditoria devem ser retidos conforme previsto na legislação no âmbito da administração pública federal.

§ 6º Os registros de logs de auditoria e outros logs de eventos de segurança devem ser revisados e retidos de maneira segura.

§ 7º A capacidade de armazenamento dos logs deve ser constantemente verificada e readequada conforme a necessidade do IFPI.

§ 8º Registros de auditoria devem ser correlacionados quando houver mais de um repositório de logs ou coletados de várias fontes de logs.

§ 9º Cópias de segurança (backups) de arquivos de trilhas de auditoria de logs devem ser armazenados de forma segura, conforme legislação pertinente.

§ 10. Quando possível, os registros devem ser armazenados conforme legislação pertinente no âmbito da administração pública federal.

Art. 35. O IFPI deve garantir que os logs de auditoria estejam disponíveis para o acesso quando for necessário, e manter o controle de acesso lógico aos diretórios onde os logs estão armazenados.

§ 1º O IFPI deve estabelecer um processo de análise de logs de eventos de

auditoria de ativos de TI considerados críticos pela ETIR de forma proativa com o objetivo de detectar possíveis anomalias de comportamento dos ativos de informação.

§ 2º A frequência, escopo e/ou profundidade da revisão, análise e relatório dos registros de auditoria devem ser ajustados para atender às necessidades do IFPI com base nas informações recebidas.

§ 3º Análises de logs de auditoria de eventos devem ser realizadas pelo menos uma vez por semana, quando possível para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.

§ 4º Processos, procedimentos e medidas técnicas devem ser definidas, implementadas e avaliadas para reporte de anomalias e falhas do sistema de monitoramento e notificação imediata ao responsável, caso confirmado.

§ 5º Eventos relacionados à segurança nos aplicativos e na infraestrutura subjacente devem ser identificados e monitorados.

§ 6º Logs e registros de auditoria de sistemas devem ser configurados e armazenados na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

§ 7º Em casos de resposta a incidentes cibernéticos, a coleta de dados forenses deve ser utilizada nos sistemas afetados, garantindo a transferência e a proteção de tais dados.

§ 8º Componentes do sistema e a operação desses componentes devem ser monitorados em busca de anomalias que sejam indicativas de atos maliciosos, desastres naturais e erros que afetem a capacidade do IFPI de atingir seus objetivos. As anomalias devem ser analisadas para determinar se representam eventos ou incidentes de segurança.

§ 9º Quando apropriado, logs de auditoria de consultas DNS e URL em ativos de informação devem ser coletados.

§ 10. As implementações de coleta de logs podem incluir a coleta de logs de auditoria de linhas de comando (CLI) tais como **PowerShell, BASH** e terminais administrativos remotos.

§ 11. O comportamento dos ativos de informação deve ser analisado para detectar e mitigar a execução de comandos e scripts que possam indicar ações maliciosas.

§ 12. Quando apropriado, logs do provedor de serviços devem ser coletados.

§ 13. Quando suportado, convém que o acesso a sistemas críticos por terceiros seja monitorado quanto a atividades não autorizadas ou incomuns.

§ 14. Processos de revisão, análise e relatórios de registros de auditoria devem ser correlacionados, para investigação e resposta a indicações de atividades ilegais, não autorizadas, suspeitas ou incomuns.

Art. 36. Os eventos de auditoria em ativos de TI considerados críticos devem ser armazenados por um período pré-estabelecido e quando este prazo vencer, o IFPI deve ser capaz de realizar a eliminação de logs de forma eficiente, com base nas melhores práticas de segurança da informação e normativos como LGPD e LAI.

§ 1º A exclusão regular de logs de auditoria de eventos considerados desnecessários deve reduzir a quantidade de dados que precisam ser filtrados para atender às requisições de resgate de informações além de reduzir os custos de armazenamento e gerenciamento de dados.

§ 2º Quando não forem mais necessários para requisitos legais, regulatórios (incluindo federais, estaduais e municipais) ou de negócios do IFPI, os dados de logs devem ser eliminados dos registros usando um método seguro aprovado.

§ 3º Quando possível deve-se implementar medidas de salvaguarda para os logs, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto, de forma que esses não tenham permissão de exclusão ou desativação dos registros (logs) de suas próprias atividades.

§ 4º A exclusão de logs de auditoria de eventos deve ser feita de modo a assegurar a irrecuperabilidade, destruindo inclusive as cópias, mídias digitais, impressos e discos rígidos.

Art. 37. Compete à alta administração:

I - prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais, estrutura organizacional e com as leis e regulamentos pertinentes; e

II - garantir recursos (humanos, tecnológicos e financeiros) para a execução de ações relacionadas ao registro de logs de auditoria no âmbito do IFPI.

Art. 38. Compete ao Comitê de Segurança da Informação:

I - deliberar sobre política e norma interna complementar de registro de logs de auditoria;

II - assessorar a implementação das ações para o registro de logs de auditoria; e

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre registro de logs de auditoria.

Art. 39. Compete à Equipe de Tratamento e Resposta a Incidentes Cibernéticos:

I - avaliar o processo de gestão de registro de logs de auditoria;

II - deliberar sobre procedimentos internos para registro de logs de auditoria; e

III - propor diretrizes e responsabilidades para a gestão de registro de logs de auditoria.

Art. 40. Compete ao Gestor de Tecnologia da Informação:

I - planejar, implementar e melhorar continuamente os controles de registro de logs de auditoria em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na Administração Pública Federal; e

II - propor diretrizes e responsabilidades para o registro de logs de auditoria.

Art. 41. Compete ao Gestor de Segurança da Informação:

I - coordenar a elaboração da política e norma interna complementar sobre registro de logs de auditoria, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

II - assessorar a alta administração na implantação da Política de Gestão de Registros (logs) de Auditoria e das normas internas de segurança da informação do IFPI;

III - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à registros de logs de auditoria;

IV - propor recursos necessários às ações de registros de logs de auditoria;

V - verificar os resultados dos trabalhos de auditoria sobre a gestão de registros de logs de auditoria; e

VI - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de registros de logs de auditoria.

Art. 42. Compete à Diretoria e demais setores de TI nas unidades do IFPI:

I - identificar os recursos, sistemas e serviços de TI que terão logs de auditoria gerenciados de acordo com a sua criticidade;

II - pesquisar, implantar e manter soluções para gestão de registro de logs de auditoria no âmbito do IFPI;

III - propor e gerenciar procedimentos de gestão de registro de logs de auditoria para a rede de comunicação de dados do IFPI;

IV - implantar, configurar, gerenciar e monitorar a estrutura de registro de logs de auditoria;

V - implementar rotinas para gestão de logs de auditoria; e

VI - definir o fluxo do processo de gestão de logs de registro de auditoria.

Art. 43. Compete aos usuários:

I - atender aos princípios e diretrizes contidos nesta política, incluindo normas e procedimentos complementares destinados à segurança da informação e comunicação; e

II - guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades.

Art. 44. Ações que violem esta política, norma interna complementar, procedimentos, ou que quebrem os controles de segurança da informação serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

Parágrafo único. Casos omissos não tratados nesta política serão submetidos ao Comitê de Segurança da Informação.

Subseção V
Da Gestão de Risco

Art. 45. O IFPI deve adotar processo de Gestão de Risco contínuo, de modo a ser atualizado periodicamente, tratando novos riscos e estabelecendo estratégias para proteção dos seus ativos de informação.

Subseção VI
Da Gestão da Continuidade

Art. 46. A DTI implementará plano de continuidade de negócios, a fim de evitar interrupções nos principais sistemas de informação do IFPI.

Subseção VII
Da Auditoria e Conformidade

Art. 47. Todos os ativos de informação, no âmbito do IFPI, são passíveis de auditoria, segundo estabelecido por norma específica.

Subseção VIII
Do Controle de Acesso

Art. 48. A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações do IFPI, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 49. Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Art. 50. Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do IFPI.

§ 1º Esta Política se aplica a todas as informações, cuja o IFPI seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento;

§ 2º Estão sujeitos a esta política todos os funcionários, sejam servidores efetivos ou temporários, do IFPI, todos os contratados e terceiros e todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do IFPI;

§ 3º A Política de Gestão de Controle de Acesso deve estar alinhada à Política de Segurança da Informação do IFPI e com a gestão de continuidade de negócios em nível organizacional.

Art. 51. O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pelo Departamento de Redes de Telecomunicações da Reitoria - DRT, baseado nas responsabilidades e tarefas de cada usuário.

§ 1º O IFPI deve implementar protocolos de comunicação e redes seguros;

§ 2º Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação;

§ 3º Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no IFPI;

§ 4º O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações;

§ 5º Deve ser utilizado o MFA para a autenticação de acesso remoto;

§ 6º O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA;

§ 7º O IFPI deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação da sua infraestrutura de rede;

§ 8º O IFPI deve adotar técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede;

§ 9º O Departamento de Redes e Telecomunicações (DRT), deve estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de departamento proprietário, data de criação/última autorização de renovação de acesso e validar todas as contas ativas do órgão, a cada 180 dias;

§ 10. O DRT deve implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade, estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente;

§ 11. O DRT deve centralizar o controle de acesso para todos os ativos de informação da organização por meio de um serviço de diretório ou provedor de SSO e definir e manter o controle de acesso dos usuários baseado em funções;

§ 12. O DRT ao conceder acesso a usuários que lidam com dados pessoais, deve-se limitar, estritamente, o acesso aos sistemas que processam esses dados ao mínimo necessário para cumprir os objetivos essenciais do processamento, em conformidade com o princípio da minimização de dados e analisando a criticamente os direitos de acesso em intervalos regulares.

Art. 52. O DRT deve implementar um processo formal de registro de usuários que tratem de dados pessoais para permitir atribuição de direitos de acesso e fornecer medidas para lidar com o comprometimento do controle de acesso do usuário, como corrupção ou comprometimento de senhas ou outros dados de registro do usuário.

§ 1º O uso de um identificador de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações;

§ 2º O uso compartilhado de identificador de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e deverá ser aprovado e documentado;

§ 3º A garantia de que o um mesmo identificador de usuário não é emitido para outros.

Art. 53. Para utilização das estações, e-mail e SUAP institucional do IFPI, será obrigatório o uso de (login) e de senha de acesso, fornecidos pela DTI, mediante solicitação formal pelo titular da unidade do requisitante.

§ 1º O formulário de solicitação de acesso se encontra disponível para preenchimento na página da diretoria: https://www.ifpi.edu.br/a-instituicao/diretorias-sistemicas/tecnologia-da-informacao que deve ser remetido à DTI por meio de processo eletrônico utilizando o balcão de serviços do Gov.Br no link: https://www.gov.br/pt-br/servicos/protocolar-documentos-junto-ao-ifpi

§ 2º Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

§ 3º Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a DTI por meio de chamado na Central de Serviços do SUAP que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 54. O login e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela DTI quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 55. O padrão adotado para o formato da conta de acesso do usuário é matricula institucional SIAPE, como por exemplo, "1234567". O padrão adotado para e-mail institucional será o primeiro nome, seguido de ponto, seguido por um sobrenome, como por exemplo, "nome.sobrenome@ifpi.edu.br".

Art. 56. O padrão adotado para o formato da senha é o definido pela DTI, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

§ 1º A formação da senha da identificação (login) de acesso à Rede Local deve seguir as regras de:

I - possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras, números e caracteres especiais;

II - recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

III - não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

IV - não utilizar termos óbvios, tais como: Brasil, senha, usuário, password ou system; e

V - não reutilizar as últimas 5 cinco senhas.

§ 2º A DTI fornecerá uma senha temporária para cada conta de e-mail criada. Esta senha deverá ser alterada pelo usuário no primeiro acesso.

Art. 57. Para o acesso a rede local e SUAP, após sua conta criada pela DTI, o usuário deve acessar o endereço <https://suap.ifpi.edu.br> e clicar na opção “Esqueceu ou deseja alterar sua senha?”, preencher as informações solicitadas e seguir as instruções encaminhadas para o e-mail pessoal ou institucional.

Art. 58. As senhas de acesso serão renovadas a cada 90 dias.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que uma nova senha seja definida.

Art. 59. A conta de acesso será bloqueada nos seguintes casos:

I - solicitação do superior imediato do usuário com a devida justificativa;

II - quando da suspeita de mau uso dos serviços disponibilizados pelo IFPI ou descumprimento da Política de Segurança da Informação – POSIC e normas correlatas em vigência; e

III - após o desligamento do usuário da instituição.

Art. 60. Quando do afastamento temporário do usuário, a conta de acesso poderá ser bloqueada a pedido do superior imediato ou da Diretoria de Gestão de Pessoas.

Art. 61. O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário a DTI.

Art. 62. A conta de acesso não utilizada há mais de 180 dias poderá ser cancelada.

Art. 63. O DRT deve garantir a implementação de um processo formal de cancelamento de contas de usuários que administrem ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir:

I - a imediata remoção ou desabilitação de usuário que tenha sido desligado do IFPI; e

II - realizar a identificação, desabilitação ou remoção periódica de contas de usuários ou de serviços que possuam identificadores semelhantes ou duplicados. Deve ser mantida apenas uma conta ativa por usuário ou serviço, evitando redundâncias. Por exemplo, um mesmo usuário não deve ter contas como “joao.silva” e “joao.silva2” ativas simultaneamente. Essa regra também se aplica a contas de serviços ou departamentais.

Art. 64. O DRT, poderá configurar o bloqueio automático de sessão nos ativos após um período de inatividade. Tal prazo pode ser específico para cada tipo de ativo.

Art. 65. O DRT deve, sempre que possível, priorizar o registro da revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

Art. 66. O IFPI deve definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências de acordo com as diretrizes a seguir:

I - definir a localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontrem dentro dos perímetros;

II - proteger os ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PINS ou cartões de acesso;

III - o IFPI deve executar testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento;

IV - os mecanismos de controle de acesso devem ser monitorados pela Pró-Reitoria de Desenvolvimento Institucional; e

V - estabelecer uma área de recepção ou outros meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

Art. 67. Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso ao setor no SUAP e à Rede Local devem ser revogados.

§ 1º O novo superior imediato ou a Diretoria de Gestão de Pessoas deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

§ 2º Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do superior imediato do antigo setor ou da Diretoria de Gestão de Pessoas.

Art. 68. O IFPI deve elaborar uma política ou normativo equivalente que defina condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto, levando em consideração as seguintes diretrizes:

I - segurança física do local de trabalho remoto; e

II - regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.

Art. 69. A utilização de identificação (login) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

§ 1º Somente os analistas e técnicos de TI do IFPI, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

§ 2º Na necessidade de utilização de login com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para a DTI, que poderá negar os casos em que entender desnecessária a utilização.

§ 3º Caso constatada alguma irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

§ 4º Excepcionalmente, poderão ser concedidas credenciais de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação da DTI.

§ 5º A DTI deve implementar o MFA para todas as contas de administrador.

§ 6º Ao tratar dados pessoais o IFPI deve observar o princípio do privilégio mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações:

I - remover os direitos de administrador nos dispositivos finais;

II - remover todos os direitos de acesso root e admin aos servidores e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento;

III - eliminar privilégios permanentes (privilégios que estão “sempre ativos”) sempre que possível;

IV - limitar a associação de uma conta privilegiada ao menor número possível de pessoas; e

V - minimizar o número de direitos para cada conta privilegiada.

Art. 70. O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados do IFPI é destinado apenas a pessoal autorizado.

Art. 71. O acesso a ambientes seguros ou ativos de tratamento e armazenamento de dados por fornecedores ou prestadores de serviços será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I - para fins específicos e autorizados;

II - autorização concedida pelo Pró-Reitoria de Desenvolvimento Institucional; e

III - supervisionado e monitorado;

Art. 72. O IFPI deve manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 73. O IFPI deve implementar e manter seguro logs ou registro físico de todos os acessos aos ativos de informação.

Art. 74. Os ativos de armazenamento e tratamento de dados que se encontrem fora do IFPI devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados conforme as seguintes diretrizes:

I - não deixar o ativo sem vigilância em locais públicos e inseguros;

II - proteger o ativo contra riscos associados a visualização de informações por outra pessoa; e

III - implementar as funcionalidades de rastreamento e limpeza remota.

Art. 75. O IFPI deve estabelecer uma política ou normativo equivalente sobre a gestão de mídias de armazenamento, de acordo com as seguintes diretrizes:

I - exigir autorização para a saída de mídias de armazenamento do IFPI;

II - armazenar mídias em local seguro de acordo com a classificação de suas informações;

III - criptografar as mídias de acordo com a classificação de suas informações; e

IV - manter cópias de segurança de mídias de acordo com a classificação de suas informações.

Art. 76. É de responsabilidade da DTI o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do IFPI.

Art. 77. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do IFPI.

§ 1º O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

§ 2º A utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

§ 3º O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 78. O usuário deve informar a DTI qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança, inclusive de terceiros.

Art. 79. É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I - não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II - evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III - interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V - não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI - utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII - não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis; e

VIII - assinar o Termo de Responsabilidade quanto a utilização da respectiva conta de acesso disponível em: https://www.ifpi.edu.br/a-instituicao/diretorias-sistemicas/tecnologia-da-informacao.

Subseção IX
Do Acesso à Internet

Art. 80. Toda a comunidade do IFPI tem direito a acessar a internet, conforme as normas especificadas nesta política, com utilização para fins acadêmicos, científicos ou administrativos, portanto esse acesso será passível de auditoria.

Art. 81. O acesso à Internet no âmbito do IFPI será concedido por meio de autenticação do usuário.

Art. 82. A DTI é responsável por implementar mecanismos de autenticação que determinem a titularidade de todos os acessos à Internet dentro da rede do IFPI.

§ 1º O acesso à internet e/ou e-mail será feito através de uso de senha, que deverá seguir as recomendações contidas no Art. 56º.

§ 2º As senhas não deverão incluir o número de matrícula, espaço entre os caracteres, partes do nome do usuário e palavras de dicionários, e não poderão ser reutilizadas quando da troca de senha.

§ 3º Nenhum usuário está autorizado a solicitar a senha de outros usuários.

§ 4º A troca de senha deverá ser feita a cada seis meses.

Art. 83. Somente a DTI/Reitoria está autorizada a criar usuários no servidor de domínio local (ifpi.int).

§ 1º A criação de contas de domínio para funcionários terceirizados deverá ser realizada por meio de abertura de chamado à DTI.

§ 2º É vedada a criação de contas de domínio para convidados.

Art. 84. A DTI/Reitoria é responsável por definir as formas de acesso aos controladores de domínio e firewall dos campi.

Subseção X
Da Gestão de Ativos da Informação

Art. 85. Os ativos da informação devem ser inventariados, classificados, documentados e revisados sempre que necessário.

Art. 86. Os ativos de cada setor, bem como sua documentação e manutenção ficarão sob responsabilidade de seu respectivo gestor.

Art. 87. A DTI manterá suporte para configuração de backup dos arquivos do usuário, ficando a gestão dos arquivos sob a responsabilidade dos proprietários.

Art. 88. Todo software instalado em dispositivo institucional deve ser devidamente licenciado, sendo proibido o uso de software que viole os direitos de propriedade do fabricante.

§ 1º Caso seja identificado o uso de software não licenciado, o usuário do dispositivo ou responsável pelo setor assume total responsabilidade em face das providências legais cabíveis.

§ 2º A DTI divulgará oportunamente lista de softwares homologados para uso no âmbito do IFPI.

Subseção XI
Da Segurança Física e do Ambiente

Art. 89. Essa sessão tem como objetivo regulamentar o controle de acesso aos Data Centers do Instituto Federal do Piauí (IFPI) e especificar os requisitos mínimos para suas instalações físicas, em conformidade com a legislação vigente:

I - data Center: Ambiente destinado ao armazenamento e processamento de dados, que requer segurança e controle rigorosos;

II - controle de Acesso: Conjunto de procedimentos e mecanismos utilizados para restringir e monitorar o acesso ao Data Center;

III - requisitos Mínimos: Padrões e condições essenciais que devem ser atendidos pelas instalações físicas do Data Center;

IV - O acesso aos Data Centers será restrito a pessoal autorizado pela DTI. Será utilizado um sistema de controle de acesso eletrônico, incluindo, mas não se limitando a, cartões de proximidade, biometria e senhas;

V - o registro de acesso aos Data Centers será mantido por um período mínimo de 2 meses;

VI - visitantes deverão ser acompanhados por um funcionário autorizado em todas as áreas do Data Center; e

VII - a DTI revisará periodicamente a lista de pessoal autorizado e os registros de acesso.

Art. 90. Os Requisitos Mínimos para Instalações Físicas de Data Center deve ser projetado com paredes, pisos e tetos resistentes ao fogo. Deve haver barreiras físicas para proteger contra acessos não autorizados. Os Data Centers devem ser equipados com sistemas de detecção e combate a incêndios, conforme normas técnicas vigentes.

Art. 91. Sistemas de monitoramento por câmeras de segurança devem ser instalados, cobrindo todas as áreas críticas.

Art. 92. Os Data Centers devem dispor de fontes de energia redundantes, incluindo gerador de emergência e sistemas de **no-break** (UPS).

Art. 93. A climatização deve ser controlada para manter a temperatura e umidade dentro dos limites recomendados para equipamentos eletrônicos com equipamentos de climatização redundantes.

Art. 94. A infraestrutura dos Data Centers deve ser inspecionada e mantida regularmente e auditorias anuais serão realizadas para assegurar a sua conformidade com esta política.

Subseção XII
Da Segurança em Recursos Humanos

Art. 95. O processo de gestão de segurança em recursos humanos será regulamentado por norma específica de acordo com a legislação vigente.

Subseção XIII
Da Gestão de Operações e Comunicações

Art. 96. A DTI, com a participação do Comitê de Segurança da Informação e Comunicação - CSIC, deve acompanhar o processo de Gestão de Operações e Comunicações desenvolvido pela ETIR, instituída em RESOLUÇÃO NORMATIVA CONSUP/OSUPCOL/REI/IFPI N° 189, de 12 de dezembro de 2023.

Subseção XIV
Da Criptografia

Art. 97. Caso se julgue necessário, as informações pertencentes ao IFPI consideradas como sigilosas poderão ser criptografadas.

Art. 98. A DTI estabelece procedimentos para criptografia de informações no âmbito do IFPI em sua política de backup.

Subseção XV
Do Desenvolvimento Seguro de Software

Art. 99. A equipe de desenvolvimento de sistemas (DSI) do IFPI (DSI) deverá passar por contínuo processo de capacitação, especialmente em boas práticas de desenvolvimento seguro.

Art. 100. Deve constar, no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do IFPI, calendário de capacitações para a equipe de TI.

Art. 101. O plano de desenvolvimento de software encontra-se publicizado em RESOLUÇÃO NORMATIVA CONSUP/OSUPCOL/REI/IFPI Nº 191, de 13 de dezembro de 2023. A sua observância deve ser levada em consideração em todo o âmbito do Instituto Federal do Piauí no que tange à implantação e desenvolvimento de sistemas informatizados.

Subseção XVI
Do Uso de E-mail

Art. 102. O e-mail Institucional será utilizado como forma de comunicação oficial entre os servidores da Instituição, sendo considerado documento comprobatório, podendo ser utilizado para fins de recebimento de ofícios, notificações, solicitações, informativos, convocações, intimações, convites, dentre outros documentos oficiais ou similares.

Art. 103. É dever do servidor verificar diariamente sua caixa de entrada do

correio eletrônico institucional.

Art. 104. A concessão de um endereço de correio eletrônico não atribui ao usuário poder de representação do IFPI.

Art. 105. Os serviços de correio eletrônico são oferecidos como um recurso para apoiar os servidores docentes e técnico-administrativos no cumprimento de suas atribuições nas áreas de administração, ensino, pesquisa, extensão, comunicação e serviços.

Art. 106. Deverá ser utilizado exclusivamente o endereço de correio eletrônico institucional em todas as atividades nas quais houver a necessidade da publicação de um endereço de correio eletrônico.

§ 1º Os atos da Administração que requeiram a Comunicação e similares, de interesse da Instituição, poderão ser realizados via e-mail institucional.

§ 2º Os servidores ficam cientes dos atos de comunicação e similares através de e-mail institucional.

Art. 107. Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética, moral e legal, devendo manter a segurança de sua conta com o uso de senhas fortes em conformidade com o Art. 56.

Art. 108. O uso do serviço de correio eletrônico institucional para fins pessoais não é priorizado, sendo permitido, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas atividades ou viole qualquer outra lei ou mesmo norma vigente no IFPI.

Art. 109. O IFPI, de forma geral, não será árbitro do conteúdo de mensagens eletrônicas com o objetivo de impedir que os usuários recebam mensagens indesejadas.

Art. 110. Listas de distribuição poderão ser criadas pelo gestor do sistema de correio eletrônico sob demanda da Instituição sem a necessidade de obtenção de permissão prévia dos usuários nelas inseridos.

Parágrafo único. É facultada ao usuário a opção de solicitar seu descadastramento da lista, ato que será analisado pela instância competente.

Art. 111. A inconveniência e possíveis ameaças contidas em mensagens indesejáveis, provenientes de fontes externas, podem levar o Administrador de Sistemas e Rede a bloquear a recepção de mensagens provenientes de alguns domínios.

Art. 112. Um endereço de correio eletrônico só poderá ser tornado público por seu detentor.

CAPÍTULO VII
DA GESTÃO DO CORREIO ELETRÔNICO

Art. 113. A cada servidor será atribuída, obrigatoriamente, uma conta de e-mail institucional a partir de seu cadastramento no sistema SUAP.

§ 1º Quanto à criação, manutenção ou remoção de conta de e-mail para servidor, aposentado e pensionista, esse procedimento será realizado e estará sob a responsabilidade da DTI/DRT ou da TI dos demais campi.

§ 2º A DTI definirá cota com capacidade limite de armazenamento de arquivos no uso da conta de e-mail. As cotas de armazenamento para uso das contas de e-mail institucional são regulamentadas por ato normativo do CONSUP.

Art. 114. O encerramento do vínculo implicará imediata notificação, e a suspensão da conta ocorrerá por 90 dias tendo sua exclusão após este prazo.

Art. 115. As contas de e-mail destinadas aos prestadores de serviços terceirizados serão criadas pela Diretoria de Tecnologia da Informação (DTI) por solicitação formal dos gestores dos contratos a que estão vinculados.

Art. 116. É obrigação dos gestores dos contratos de que trata o item anterior a comunicação formal à DTI do encerramento do vínculo desses prestadores de serviços com o IFPI para fins de encerramento da conta de e-mail.

Art. 117. O encerramento da conta de e-mail de que trata o Artigo 105, implicará imediata suspensão da mesma. Os arquivos vinculados a essa conta ficarão disponíveis para retirada por seu detentor por um período de 60 (sessenta) a 90 (noventa) dias contados a partir da data do encerramento do vínculo. Encerrado esse período, os arquivos serão descartados.

Art. 118. As contas de e-mail não previstas neste documento poderão ser criadas por solicitação formal do Gabinete da Reitoria, das Pró-Reitorias e Diretorias de Campi à DTI, que deverão informar também o final do vínculo para efeito de encerramento da conta.

Art. 119. As contas de e-mail destinadas aos alunos do IFPI serão criadas pela TI dos campi. Quando criadas, uma senha padrão será definida, exigindo-se que o aluno a altere no primeiro acesso à conta de e-mail.

§ 1º A manutenção de conta de e-mail de aluno, como alteração de senha, problemas de acesso, ficará sob a responsabilidade da TI dos campi do IFPI.

§ 2º A DTI manterá a análise de contas de e-mail e, havendo identificação de alunos que já tenham colado grau ou com matrícula cancelada, a Diretoria de TI procederá à exclusão dessa conta.

§ 3º Em caso de aluno com matrícula cancelada ou que já tenha colado grau, a DTI notificá-lo-á sobre a exclusão da conta de e-mail. A partir dessa notificação, o aluno terá um prazo de até 15 dias para proceder aos backups de sua conta de e-mail.

§ 4º Por motivo de limitação do Google Workspace, a conta de e-mail já excluída apenas poderá ser recuperada no prazo de até 90 dias.

§ 5º As contas de e-mail de alunos seguirão, obrigatoriamente, o padrão “sigladocampus.matricula@aluno.ifpi.edu.br”.

§ 6º O identificador de matrícula tem que ser exatamente igual ao sistema acadêmico. O que divergir serão padrões legados que não podem ser replicados a partir da publicação deste documento.

§ 7º As contas de e-mail de servidores seguirão, preferencialmente, o padrão “nome.sobrenome@ifpi.edu.br”, conforme Padrão de Formação de Endereços de Correio Eletrônico - 2020.

§ 8º As contas de e-mail de setores e/ou comissões seguirão, preferencialmente, o padrão “siglasetor.sigladocampus@ifpi.edu.br”.

§ 9º Todos os usuários do correio eletrônico devem implementar o duplo fator de segurança para efetuar logon em sua conta.

CAPÍTULO VIII
DA PRIVACIDADE DO E-MAIL INSTITUCIONAL

Art. 120. A divulgação massiva de mensagens só poderá ser feita pelas instâncias de comunicação social do IFPI.

Art. 121. As mensagens de correio eletrônico, no domínio "ifpi.edu.br", na condição de arquivos armazenados ou gerados com os recursos da Diretoria de Tecnologia da Informação (DTI), para fins produtivos, também são de propriedade do IFPI e, portanto, passíveis de auditorias.

Art. 122. A auditoria a que faz referência o artigo anterior destina-se exclusivamente à manutenção da segurança da infraestrutura de Tecnologia da Informação e Comunicação (TIC), bem como ao resguardo dos objetivos institucionais.

Art. 123. Fica assegurado aos usuários o sigilo de conteúdo de seus e-mails e arquivos, exceto por determinação judicial em contrário ou por força de Sindicância ou ainda Processo Administrativo Disciplinar.

Art. 124. À DTI fica assegurado o direito de, em casos nos quais a segurança dos recursos de TIC da Instituição sejam ameaçados, eliminar contas de correio eletrônico, mensagens e arquivos, bloquear conteúdos e usuários, temporariamente ou permanentemente.

CAPÍTULO IX
DAS PROIBIÇÕES

Art. 125. Os usuários do serviço de correio eletrônico não podem:

I - falsificar sua identidade ou o seu nome de usuário ao utilizar o sistema de mensagens ou alterar a linha de origem da mensagem ou qualquer outra indicação de sua origem;

II - iniciar ou reenviar mensagens encadeadas (correntes);

III - gerar boatos (hoax), mensagens com objetivos de obtenção indevida de informações (phishing) ou qualquer outra atividade que viole o disposto nesta POSIC;

IV - praticar crimes e infrações de qualquer natureza, por meio do sistema de correio eletrônico do IFPI;

V - executar ações nocivas contra outros recursos computacionais do IFPI ou de redes externas;

VI - distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, difamatório ou de qualquer forma contrário ao Regime Jurídico Único Brasileiro;

VII - divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço correio eletrônico institucional; e

VIII - praticar quaisquer atividades lesivas, as quais tendem a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

CAPÍTULO X
DAS PENALIDADES

Art. 126. Reserva-se à DTI o direito de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet. Qualquer descumprimento desta política será tratado como incidente de segurança e poderá implicar aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente ou em qualquer outra

legislação que regule ou venha a regular a matéria.

Art. 127. Uma vez detectada violação da política, determina-se a sua causa, que pode ser por:

I - negligência;

II - acidente;

III - erro; ou

IV - ação previamente determinada, ignorando a POSIC estabelecida.

Parágrafo único. Técnicos da DTI identificarão os usuários, violadores do caput deste artigo.

Art. 128. Se for provado que o usuário violou os preceitos existentes nesta política e nos documentos elaborados a partir dela, a Controladoria/Corregedoria ficará responsável, quando provocada, para a abertura de Processo Administrativo Disciplinar, com o objetivo de apurar o desvio de conduta do servidor, garantindo o contraditório e a ampla defesa.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 129. Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário.

Art. 130. Os casos omissos serão julgados pelo Comitê de Segurança da Informação e Comunicações.

Art. 131. Fica revogada a Resolução Normativa nº 127/2022 – CONSELHO SUPERIOR, de 7 de abril de 2022.

Art. 132. Esta Resolução entra em vigor na data de sua publicação.

PAULO BORGES DA CUNHA
Presidente do CONSUP

Documento assinado eletronicamente por:

- **Paulo Borges da Cunha**, **REITOR(A) - CD1 - REI-IFPI**, em 19/12/2024 15:11:33.

Este documento foi emitido pelo SUAP em 16/12/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpi.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 318565
Código de Autenticação: ed73f12bf4