



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

RESOLUÇÃO CONSU/IFAC Nº 009, DE 10 DE JANEIRO DE 2019

Dispõe sobre a Política de Segurança da Informação e Comunicação de Dados no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Acre.

O Presidente Substituto do Conselho do Instituto Federal de Educação, Ciência e Tecnologia do Acre (IFAC), no uso de suas atribuições legais, conferidas pelo artigo 12 da Lei nº 11.892, de 29/12/2008, nomeado pela portaria nº 635 de 07 de maio de 2018, publicada no Diário Oficial da União nº 87 de 08 de maio de 2018, seção 2. Considerando o deliberado na 25ª Reunião Ordinária do Conselho Superior, no dia 07/12/2018, o que consta no inciso III, do artigo 9º e no artigo 39, da Resolução CONSU/IFAC nº 045, de 12/08/2016, que aprova o Regimento Interno do Conselho Superior, considerando o Processo nº 23244.014647/2018-99,

Considerando 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

Considerando a Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta

Considerando a Norma complementar 03/IN01/DSIC/GSIPR de 30 de junho de 2009, trata das diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;

Considerando a Portaria nº 19, de 29 de maio de 2017, da Secretaria de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão, que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP;

Considerando a Resolução CONSU/IFAC nº 050/2017 de 18 de dezembro de 2017, que institui o Comitê Gestor de Segurança da Informação e Comunicações;

Considerando a Portaria nº 946, de 28 de junho de 2018, que atualiza os membros do Comitê Gestor de Segurança da Informação e Comunicações;

Considerando a necessidade de atualizar a atual Política de Segurança da Informação do IFAC;



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

RESOLVE:

Art. 1º Aprovar a nova Política de Segurança da Informação e Comunicação de Dados – POSIC;

Art. 2º Revogar a Resolução nº 46, de 18 de outubro de 2011;

Art. 3º Esta Resolução entra em vigor na data da publicação.

Rio Branco/AC, 10 de janeiro de 2019.

(Original assinado)

UBIRACY DA SILVA DANTAS
Presidente do Conselho Superior Substituto



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

ANEXO

EQUIPE DE ELABORAÇÃO E COLABORAÇÃO

Keyla Oliveira da Silva	Coordenadora de Gestão de Tecnologia da Informação
Djameson Oliveira da Silva	Diretor de Gestão de Tecnologia da Informação
Aysilon Melo da Silva	DSGTI/COGTI
Ricardo Yamasaki Sassagawa	DSGTI/COSIS
Kellyton de Almeida Azevedo	DSGTI/COSEG
Saulo Maia de Freitas	DSGTI/COSIN
Helson da Silva Santana Ferreira	DSGTI/COSIN
Giuliano Cardoso Feitosa Miranda	DSGTI/COSIS
José Jair Cavalcante de Figueiredo	DSGTI/COSIS
Victor Moreno dos Santos Galdino	DSGTI/COSEG

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
27/08/2018	1.0	Versão aprovada pelo Comitê Gestor de segurança da Informação e Comunicações
30/11/2018	1.1	Versão aprovada pelo CONSU

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DE DADOS
DO INSTITUTO FEDERAL DO ACRE - POSIC/IFAC**

**CAPÍTULO I
VISÃO GERAL**

A Política de Segurança da Informação e Comunicação de Dados - POSIC é constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento dos ativos e informações processadas, armazenadas ou custodiadas pelo Instituto Federal do Acre - IFAC;

Para fins desta instrução, considera-se Segurança da Informação o conjunto de políticas, normas e procedimentos que objetivam o controle de acesso, à preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade, integridade dos ativos, dados e responsabilidade das informações e dos Recursos de Tecnologia da Informação - RTI.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

As diretrizes estabelecidas nesta Política de Segurança da Informação e Comunicação de Dados determinam os parâmetros que devem ser seguidos pelo IFAC para que sejam assegurados todos os recursos computacionais e informações de seu domínio.

OBJETIVO

Normatizar a utilização dos recursos computacionais, das informações e serviços pertinentes ao IFAC para garantir os princípios fundamentais da segurança da informação, visando a proteção dos processos e imagem institucional.

ABRANGÊNCIA

Esta Política de Segurança da Informação e Comunicação de Dados é aplicável a todos os bens e serviços e a todo o pessoal que se utiliza dos Recursos de Tecnologia da Informação - RTI, no âmbito do IFAC, incluindo:

- I.** Informações impressas, manuscritas ou armazenadas de forma digital;
- II.** Correio eletrônico de domínio do IFAC;
- III.** Informações processadas por quaisquer dispositivos eletrônicos dentro do domínio do IFAC;
- IV.** Reuniões e comunicados realizados por qualquer meio de comunicação digital.

INSTÂNCIAS ADMINISTRATIVAS

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

- I.** Políticas de Segurança da Informação e Comunicação (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;
- II.** Comitê Gestor de Segurança da Informação e Comunicação - CGSIC: comitê responsável por elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicação de Dados e normas relacionadas, submetendo à aprovação do Conselho Superior do IFAC, entre outras competências;
- III.** Diretoria Sistêmica de Gestão da Tecnologia da Informação (DSGTI): órgão executivo vinculado à reitoria, que planeja, executa, instrui, supervisiona e mantém a funcionalidade das tecnologias da informação, com articulação entre as atividades de ensino, pesquisa e extensão no IFAC e atendimento às necessidades gerais da Reitoria e dos campi no que se refere às suas competências.
- IV.** Coordenação da Tecnologia da Informação e Comunicação - CORTI: Órgão Executivo vinculado a Diretoria de Administração de cada campus.

CONCEITOS

Para fins dessa política considera-se:



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

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

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

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

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

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

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

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

Dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

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;

Risco: combinação da probabilidade de ocorrência de um evento e de suas consequências;

Gestão de riscos: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para mitigar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos;

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

Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

Avaliação de riscos: processo onde se compara o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;

Análise/avaliação de riscos: processo completo de análise e avaliação de riscos;

Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco;

Aceitação do risco: decisão de aceitar a probabilidade de ocorrência de eventos ou incidentes de segurança e suas consequências;

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação desta Política de Segurança da Informação e





MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Comunicação de Dados ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para segurança da informação [ISO/IEC TR 18044:2004];

Incidente de segurança da informação: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004];

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição [ISO/IEC 13335-1:2004];

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

Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição. Neles incluem-se:

- a) Ativos de informação;
- b) Ativos de software;
- c) Ativos físicos;
- d) Serviços;
- e) Pessoas e suas qualificações, habilidades e experiências;
- f) Reputação e a imagem da instituição.

Ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

Ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

Recursos de Tecnologia da Informação (RTI): os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados nas Unidades de Ensino, tais como:

- a) Equipamentos de informática e de telecomunicações de qualquer espécie;
- b) Infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;
- c) Laboratórios de informática de qualquer espécie; e
- d) Recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação, programas de computador, arquivos de configuração que são armazenados, executados e/ou transmitidos por meio da infraestrutura computacional do IFAC, redes ou outros sistemas de informação.

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

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

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;



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

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;

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulte no comprometimento da Segurança da Informação;

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

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;

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

Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e/ou equipamentos que estejam vinculados administrativamente ao IFAC;

Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e/ou equipamentos que não esteja vinculada administrativamente ao IFAC;

Comunicação oficial: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IFAC, de atividades especiais ou ainda de projetos específicos;

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.

PRINCÍPIOS

Além dos princípios de confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, esta Política de Segurança da Informação e Comunicação de Dados baseia-se também nos seguintes princípios:

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

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 IFAC são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação e Comunicações advindas desta política;

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;

Ética: Todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFAC devem ser respeitados;

Legalidade: Além de observar os interesses do IFAC, as ações de Segurança da Informação levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e direitos de uso;

Proporcionalidade: O nível, a complexidade e os custos das ações de Segurança da Informação no IFAC serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

DAS FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

Constituição Federal de 1988;

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;

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;

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;

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

Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta
Norma complementar 03/IN01/DSIC/GSIPR de 30 de junho de 2009, trata das diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;

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

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

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

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;

Outros dispositivos legais aplicáveis, a saber:

Norma complementar nº 01/IN01/DSIC/GSIPR, de 13 de outubro de 2008;

Norma complementar nº 02/IN01/DSIC/GSIPR, de 14 de outubro de 2008;

Norma complementar nº 03/IN01/DSIC/GSIPR, de 3 de julho de 2009;

Norma complementar nº 04/IN01/DSIC/GSIPR, de 17 de agosto de 2009;



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Norma complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009;
Norma complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009;
Lei nº 7.232, de 29 de outubro de 1984, que dispõe sobre a Política Nacional de Informática;
Norma ISO/IEC GUIDE nº 51:1999, que fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

DA DECLARAÇÃO DE COMPROMETIMENTO DA REITORIA

A alta direção do IFAC, na figura da Reitora, declara-se comprometida em proteger todos os seus ativos de informação.

REVISÃO E ATUALIZAÇÃO

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

CAPÍTULO II **DIRETRIZES GERAIS**

Art. 1º O servidor público, estagiário e colaboradores usufruindo os ativos do IFAC são responsáveis por prezar pela segurança da informação dentro da instituição, especialmente por aquelas que estão sob sua tutela e usabilidade;

Art. 2º O IFAC sendo uma unidade parceira e cliente dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatário de suas Políticas e Normas de Segurança;

Art. 3º Os usuários internos e externos devem observar que:

- I.** O acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFAC é considerada seu patrimônio e deve ser protegida;
- II.** Os recursos tecnológicos disponibilizados pelo IFAC, são fornecidos com o propósito único de garantir o desempenho das suas atividades;
- III.** As normas para as operações de armazenamento, divulgação, reprodução, recuperação e destruição da informação serão definidas de acordo com a classificação desta, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor;
- IV.** O serviço de correio eletrônico 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 IFAC e, portanto, passível de auditoria;
- V.** Todo acesso à Internet será monitorado e passível de auditoria.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

- VI.** Será concedida permissão de acesso aos recursos da rede de computadores a estagiários e funcionários de empresas contratadas pelo IFAC, mediante solicitação formal dos titulares das unidades onde estejam lotados, com limitações às necessidades do serviço.
- VII.** As permissões de acesso a cada recurso deverão ser retiradas por SOLICITAÇÃO realizada através de sistemas de chamados técnicos pelo responsável da unidade de lotação do servidor, dos estagiários e dos funcionários de empresas contratadas, quando não utilizadas adequadamente ou quando desligados dos quadros do Instituto Federal do Acre.
- VIII.** Não é permitido acesso sem autorização aos recursos da rede de computadores, através de roubo de credenciais ou da exploração de vulnerabilidades de segurança de qualquer servidor, rede ou conta.
- IX.** Acesso à Internet/Intranet e o envio e recebimento de correio eletrônico por meio dos equipamentos e serviços do Instituto Federal do Acre destinam-se às necessidades dos serviços institucionais.
- X.** O servidor que apagar, destruir ou modificar programas ou arquivos de sistemas ou, de qualquer forma, inutilizar, total ou parcialmente equipamentos RTI, ou ainda, fizer uso, de forma indevida ou não autorizada, dos equipamentos de informática terá seu acesso ao serviço de redes de comunicação de dados suspenso, seguido das demais sanções administrativas, civis e penais, conforme o caso.
- XI.** A suspensão será comunicada ao superior imediato do usuário, através de notificação, e o seu restabelecimento somente ocorrerá mediante análise do Comitê Gestor de Segurança da Informação e Comunicação - CGSIC;
- XII.** É proibida a exploração de falhas ou vulnerabilidades porventura existentes nos ativos de informação do Instituto Federal do Acre.
- XIII.** Os casos omissos e necessários ao bom tráfego de informações na rede de computadores do Instituto Federal do Acre serão cuidadosamente analisados pela DSGTI que, em qualquer caso, procederá sem violação dos preceitos legais e desta Resolução.
- XIV.** A DIRETORIA SISTÊMICA DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO – DSGTI procederá o bloqueio do acesso ou cancelamento da conta de usuário caso seja detectado uso em desconformidade com o estabelecido nesta política e será aplicado as sanções estabelecidas no Capítulo XII das Sanções Administrativas.
- XV.** Os parâmetros de configuração dos computadores serão definidos pela DSGTI, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional do IFAC.
- XVI.** Incluem-se nas definições os serviços disponíveis por meio da internet e intranet.
- XVII.** Não serão autorizadas modificações efetuadas em parâmetros dissonantes das definições estabelecidas.

CAPÍTULO III
DA SEGURANÇA DA INFORMAÇÃO

Art. 4º Os sistemas de informação e os serviços de rede do IFAC serão classificados em três níveis quanto à segurança:



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

§ 1º Disponibilidade – indica o quanto um sistema de informação ou serviço de rede deve estar disponível para acesso do usuário. Quanto à disponibilidade, os sistemas de informação e os serviços de rede são classificados como:

I. De alta disponibilidade: com indisponibilidade máxima de 2h (duas horas) ininterruptas no período das 8 às 18h em dias úteis (assim considerados os dias com atividades administrativas nos setores da Administração Central do IFAC) e 24h (vinte e quatro horas) ininterruptas fora deste período. São considerados sistemas e serviços de alta disponibilidade: o acesso ao correio eletrônico e ao portal institucional (www.ifac.edu.br);

II. De média disponibilidade: com indisponibilidade máxima de 4h (quatro horas) ininterruptas no período das 8 às 18h em dias úteis e 48h ininterruptas fora deste período. São considerados sistemas e serviços de média disponibilidade: todos os sistemas de informação (acadêmicos e administrativos) hospedados nas máquinas servidoras de responsabilidade da DSGTI e os serviços de rede também hospedados nas máquinas servidoras de responsabilidade da DSGTI e que não estão enquadrados como de alta disponibilidade;

III. De baixa disponibilidade: sem definição de tempo de indisponibilidade. São considerados sistemas e serviços de baixa disponibilidade: os sistemas de informação e serviços de rede não hospedados nas máquinas servidores de responsabilidade da DSGTI como SERPRO, SIAF, SIASG, SIAPENET dentre outros.

§ 2º Confidencialidade – indica a permissão de acesso à informação. Quanto à confidencialidade, os sistemas de informação e os serviços de rede são classificados como:

a) confidenciais: de acesso restrito a usuários autorizados nominalmente. São considerados sistemas e serviços confidenciais: todos os sistemas de informação (acadêmicos e administrativos), o correio eletrônico institucional, os repositórios de arquivos, os serviços de banco de dados, os módulos de administração e configuração dos sistemas e serviços de circulação restritos ou abertos;

b) de circulação restrita: de acesso permitido a todos os usuários cadastrados no domínio de rede, podendo haver diferenciação por perfil de usuário. São considerados sistemas e serviços de circulação restrita: serviços, aplicações e conteúdos institucionais direcionados aos usuários cadastrados (Intranet), modelos de documentos e formulários web, arquivos de uso geral, serviços de impressão;

c) abertos: de acesso livre apenas para leitura. São considerados sistemas e serviços abertos: websites e sistemas de consulta pública.

§ 3º Integridade – indica o grau de importância de manutenção de cópias de segurança. Quanto à integridade, às informações e serviços de rede são classificados como:

a) integridade alta: que prevê redundância de gravação para recuperação integral da última informação armazenada em caso de sinistro, cópia de segurança diária e guarda de informações de datas anteriores. São considerados sistemas e serviços de alta integridade: todos os sistemas de informação (acadêmicos e administrativos) hospedados nas máquinas servidoras de responsabilidade da DSGTI, o correio institucional e as configurações e scripts de serviços;

b) integridade média: que prevê cópia de segurança diária e guarda de informações de datas anteriores. São considerados sistemas e serviços de média integridade: os serviços de



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

rede hospedados nas máquinas servidoras de responsabilidade da DSGTI que não estão enquadrados como de alta integridade;

c) sem garantia: que não prevê guarda de dados. São considerados sistemas e serviços sem garantia: os serviços, sistemas e informações não hospedados nas máquinas servidoras de responsabilidade da DSGTI e que não possuem cópia de segurança diária em máquina servidora de responsabilidade da DSGTI, os serviços e informações relacionados a alunos e visitantes, os arquivos guardados em sistemas que não são as máquinas servidoras da DSGTI (estações de trabalho, pen drives, e outros), demais informações não citadas anteriormente.

Art. 5º Todos em consonância com o CGSIC são responsáveis pela garantia da segurança da informação no âmbito do IFAC.

CAPÍTULO IV
DO ACESSO AOS SERVIÇOS

Art. 6º O acesso aos recursos da rede de computadores é garantido a todos os servidores do Instituto Federal do Acre e colaboradores autorizados, com utilização exclusiva para fins diretos e complementares às atividades do setor com as devidas limitações inerentes ao cargo e a unidade de lotação.

Art. 7º O acesso aos recursos da rede de computadores e demais ativos é garantido a todos os alunos com utilização para fins acadêmicos e/ou atividades que não infrinja esta Política de Segurança da Informação e Comunicação de Dados.

Art. 8º A DSGTI disponibiliza vários serviços de rede ao usuário, sendo que, para obter acesso, é necessária a criação de contas de acesso, que serão compostas por um usuário (nome de usuário) e uma senha de uso pessoal e intransferível.

Art. 9º Quando solicitado via sistema de abertura de chamado, a criação das contas de usuários para todos os sistemas de acordo com o seguinte padrão:

Art. 10 O nome de usuário será composto pelo primeiro nome e pelo último sobrenome, separados por um ponto (.). Se o sistema acusar a existência deste nome de usuário será usada a primeira letra de outro sobrenome (ou nome do meio) seguido do último sobrenome e assim por diante. Exemplo: Para o servidor Fulano Rosário dos Ventos, será criado o usuário fulano.ventos. Caso já exista este nome de usuário, será então criado fulano.rventos. Nos casos específicos nos quais os padrões definidos por este artigo forem impraticáveis, ficará a DSGTI juntamente com o usuário em questão responsável por estipular a melhor opção.

Parágrafo único. Será criada uma senha provisória para o usuário, que deverá ser alterada na primeira utilização. Para alteração da senha de cada serviço o servidor deverá consultar os tutoriais disponíveis no portal do IFAC na área específica da DSGTI. A nova senha deverá seguir o padrão descrito na política de senhas.

Art. 11 O acesso aos serviços deverá ser solicitado pela chefia imediata, através do sistema de abertura de chamado (chamados.ifac.edu.br) para a criação dos novos usuários ou acesso a serviços com restrições.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 12 A solicitação de criação de novos usuários deverá conter as seguintes informações comprovadas através de cópia de documento em anexo ao chamado:

- I. Nome completo do Servidor;
- II. Data de nascimento;
- III. CPF;
- IV. Cargo;
- V. Local de lotação.

Art. 13 O servidor que desejar acesso aos módulos do sistema SIG, deverá solicitar à sua chefia imediata que requisite através do sistema de abertura de chamado.

Art. 14 A solicitação de criação de novos usuários no Sistema SIG deverá conter as seguintes informações comprovadas através de cópia de documento anexado ao chamado:

- I. Nome completo do Servidor;
- II. Data de nascimento;
- III. CPF;
- IV. Portaria com data de nomeação do cargo;
- V. Local de lotação;
- VI. Descrição dos módulos que queira ter acesso;
- VII. Justificativas.

Art. 15 Será disponibilizado acesso à internet aos visitantes do Instituto Federal do Acre para fins institucionais mediante cadastro prévio e justificativa. O cadastro deverá conter as seguintes informações:

- I. Nome completo;
- II. Data de nascimento;
- III. CPF;
- IV. Período de acesso;
- V. Justificativa do acesso.

§ 1º O cadastro deverá ser realizado por um servidor da respectiva unidade de lotação onde ocorrerá o acesso.

§ 2º O uso indevido do acesso por parte do visitante é de sua total responsabilidade, se detectado, o visitante deverá ter seu acesso bloqueado.

Parágrafo único. As informações referentes aos acessos, usuário e senha dos servidores, serão repassadas através do sistema de chamado técnico.

Seção I Políticas de Senhas

Art. 16 As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese. Tudo que for executado com a sua senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

§ 1º Manter sob sua guarda sua senha pessoal, evitando deixá-la a vista ou repassá-la a outras pessoas, sendo de sua responsabilidade o mau uso desta por qualquer pessoa;

§ 2º Não utilizar quaisquer programas ou dispositivos para interceptar ou decodificar senhas ou similares;

§ 3º Não utilizar senhas de terceiros obtidos por qualquer meio;

§ 4º A alteração de senhas deverá obedecer aos seguintes critérios:

a) a senha deverá ser composta por no mínimo 7 (sete) e no máximo 12 (doze) caracteres contendo letras, números e possivelmente caracteres especiais;

b) a senha não deve conter partes do nome da pessoa ou dados pessoais como data de nascimento, CPF ou RG;

c) a senha poderá ser composta por uma combinação de letras maiúsculas, minúsculas, numerais e caracteres especiais.

§ 5º A senha deverá ser redefinida pelo menos a cada seis meses, para usuários comuns. As senhas devem ser bloqueadas após 5 (cinco) tentativas sem sucesso, sendo que, o administrador da rede e o usuário devem ser notificados sobre estas tentativas.

§ 6º Para mais dicas sobre como criar senhas seguras acesse o seguinte documento: <https://cartilha.cert.br/fasciculos/senhas/fasciculo-senhas-slides.pdf>

CAPÍTULO V
DA POLÍTICA DE UTILIZAÇÃO DE E-MAIL INSTITUCIONAL
Seção I
Das normas para utilização do e-mail institucional

Art. 17 Este capítulo define as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento das contas de e-mail, devendo ser observadas pelos servidores, alunos e colaboradores.

Art. 18 A veiculação de mensagens de conteúdo deve ser de uso exclusivamente, acadêmico ou administrativo; não sendo permitido o uso para fins comerciais, políticos, religiosos, enfim, que não seja consonante com o uso institucional.

Art. 19 É inadmissível o uso do e-mail institucional do IFAC para transmissão e recebimento de mensagens pessoais do usuário, bem como para acesso a redes sociais, cadastros em sites de compras bem como qualquer outra utilização que diverge das funções institucionais.

Art. 20 Os serviços de e-mail do IFAC são caracterizados como um recurso profissional para apoiar os usuários cadastrados no cumprimento dos objetivos institucionais, portanto devem merecer o mesmo tratamento da correspondência impressa.

Art. 21 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 IFAC, salvo para finalidade institucional.

Art. 22 A DSGTI não se obriga a garantir a inviolabilidade absoluta das mensagens eletrônicas que trafegarem no e-mail institucional.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 23 O e-mail institucional será fornecido pelo IFAC a todos os servidores da instituição.

Art. 24 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 IFAC.

§ 2º 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.: lista de e-mails de docentes.

Art. 25 O acesso às contas de e-mail será realizado via webmail, aplicativo para dispositivos móveis ou clientes POP e IMAP.

Art. 26 Compete ao chefe de setor solicitar a criação da conta de e-mail institucional de um servidor.

Art. 27 Compete ao chefe de departamento solicitar a criação da conta institucional vinculada ao departamento, bem como vincular e desvincular usuários a esta conta.

Art. 28 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. 29 Compete a Diretoria Sistêmica de Gestão de Pessoas - DISGP INFORMAR via sistema de abertura de chamado sobre o desligamento/EXONERAÇÃO de servidores, estagiários e colaboradores 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 realizada através do sistema de abertura de chamado.

Art. 30 O servidor desligado do IFAC terá um período de 5 dias para reencaminhar suas mensagens para outra conta de e-mail pessoal ou institucional ao qual está vinculado, após este período, sua conta será bloqueada.

Art. 31 O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada ou tamanho das mensagens.

Art. 32 No recebimento de e-mails, o Instituto Federal do Acre fará uso de ferramentas especializadas a fim de reduzir a incidência de spams, e de remover qualquer conteúdo considerado impróprio ou indevido.

§ 1º É proibido o envio de grande quantidade de mensagens de e-mail (spam) que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como: publicidade, comercial ou não, anúncios e informativos, propaganda política, correntes, e-mail de cunho religioso, conteúdo racista ou qualquer outro conteúdo que não seja de cunho do IFAC.

§ 2º É proibido o envio de e-mail mal-intencionado ou e-mail que sobrecarregue a caixa de e-mail dos usuários e/ou servidores (equipamento).

Art. 33 A privacidade no acesso à Internet/Intranet e no uso do correio eletrônico é garantida, mas os endereços acessados serão registrados, e o conteúdo das mensagens poderá ser rastreado ou varrido, de forma automática, por softwares especiais para verificar a adequação de seu conteúdo às normas estabelecidas nesta Resolução.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 34 O envio de mensagens, imagens ou notas a todos os componentes da lista de endereços do Instituto Federal do Acre fica restrito a assuntos de interesse geral dos servidores, sendo seu conteúdo de responsabilidade das unidades credenciadas na DSGTI, previamente autorizadas pela Diretoria Sistêmica de Comunicação, para tal finalidade.

§ 1º Poderá ser criada lista parcial de destinatários, desde que o conteúdo das mensagens, das imagens ou das notas enviadas seja compatível com as atribuições do servidor.

§ 2º Cabe à DSGTI estipular os limites de utilização do correio eletrônico necessários para o bom funcionamento do serviço, incluídos os de quantidade de destinatários, tamanho máximo das mensagens enviadas e da caixa postal e tipos permitidos de arquivos anexos.

Art. 35 É vedado aos servidores, prestadores de serviço e estagiários passar ou repassar mensagens ofensivas à honra de pessoas, órgãos ou instituições públicas e privadas, sob pena de sofrer sanções administrativas e penais.

Art. 36 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, 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 IFAC, servidores ou terceiros, e que não tenham finalidade amparada pela legislação.

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



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

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

Art. 37 Arquivos anexos nas mensagens recebidas poderão ser bloqueados de acordo com a sua extensão (tipo de arquivo) e/ou seu tamanho.

Seção II
Das recomendações para uso do e-mail institucional

Art. 38 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 a 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 DSGTI sobre o recebimento constante de e-mail não solicitado por parte do usuário;
- VIII.** Informar à DSGTI sobre qualquer ação suspeita que venha ocorrer com sua conta de e-mail.
- IX.** Os documentos oficiais devem, sempre que possível, ser enviados em formato .PDF, .DOC ou ODT.
- X.** Não permitir acesso de terceiros à sua conta de correio eletrônico;
- XI.** Atualizar seus dados cadastrais utilizando os meios disponíveis.
- XII.** Somente clientes de correio eletrônico homologados pela DSGTI devem ser utilizados.
- VXIII.** Utilizar o campo de cópia oculta (BCC/CCO) do cliente de correio eletrônico sempre que for enviada uma mensagem para mais de um destinatário.
- VIX.** Não fazer uso do correio eletrônico funcional em Listas de Discussão com assuntos não relacionados à atividade profissional.
- XVI.** Será permitido o envio de e-mail em massa somente por contas de e-mails setoriais da alta administração tais como: pró-reitorias, diretorias gerais dos campi, diretorias sistêmicas e setores de assessoramento, caso haja necessidade devidamente justificada. Em hipótese nenhuma por contas individuais, comissões ou conselhos.

Seção III
Das formatações de contas do e-mail institucional

Art. 39 As contas dos servidores públicos ativos deverão obedecer a seguinte formatação: nome.sobrenome@ifac.edu.br

Parágrafo único. A conta de usuário individual criada para o servidor é de sua própria responsabilidade.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 40 A identificação dos departamentos terá o prefixo de identificação do campus ao qual pertença, sendo assim identificados:

- I.** CBS – Campus Rio Branco Avançado Baixada do Sol;
- II.** CCS – Cruzeiro do Sul;
- III.** CRB – Campus Rio Branco;
- IV.** CSM – Campus Sena Madureira;
- V.** CTA – Campus Tarauacá;
- VI.** CXA – Campus Xapuri.

§ 1º As contas dos departamentos deverão obedecer à seguinte formatação: prefixo do campus.setor@ifac.edu.br

§ 2º As contas de usuário institucionais criadas para os Setores, Diretorias e Pró-Reitorias são de responsabilidade dos titulares das respectivas funções.

§ 3º Os Departamentos existentes apenas na Reitoria e os sistemas que sejam de âmbito do IFAC, 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. 41 As contas dos serviços devem ter o prefixo do campus seguido da identificação do serviço. Ex: crb.ccc@ifac.edu.br.

Art. 42 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: cbs.jifac@ifac.edu.br.

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

Seção IV

Dos deveres e responsabilidades do usuário

Art. 43 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 sistema de abertura de chamado técnico, que está disponível no endereço chamados.ifac.edu.br.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 44 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. 45 São deveres do administrador das contas de e-mail:

- I.** Disponibilizar a utilização do e-mail institucional aos servidores do IFAC, 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 – IFAC sobre interrupções previsíveis desses serviços;
- III.** Prestar esclarecimentos aos servidores do IFAC, 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, quando solicitado;
- 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.

CAPÍTULO VI

DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO – RTI

Art. 46 A Diretoria Sistêmica de Tecnologia da Informação - DSGTI se reserva o direito de monitorar o tráfego e o conteúdo das redes de comunicação do IFAC.

§ 1º A DSGTI em conjunto com CGSIC são também responsáveis:

- I.** Pela aplicação e fiscalização da Política de Segurança da Informação e Comunicação de Dados no IFAC;
- II.** Por implementar, por meio da expedição de atos normativos complementares, a aplicação dessa política.

§ 2º Toda solicitação de suporte (Instalação, prevenção e correção) ao usuário deverá ser feita através de um serviço Web para abertura e acompanhamento de chamados, além da definição de Acordos de Nível de Serviço - SLA (*Service Level Agreement*) - fixando prazos de atendimento (TA) e de solução (TS) das requisições.

§ 3º Fica terminantemente proibido a alteração e/ou mudança de lugar ou setor de qualquer equipamento que constituem os recursos tecnológicos desta instituição sem autorização prévia



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

da DSGTI na Reitoria ou pelas CORTIs nos campi e havendo autorização de mudança, deverá ser comunicado imediatamente ao setor de patrimônio do instituto.

§ 4º Fica assegurada a DSGTI e CORTIs na intervenção e atendimento das requisições registradas, a utilização de meios tecnológicos que assegurem resolução do problema mais rapidamente, com menor esforço administrativo, tais como funções ou softwares de acesso remoto, i.e. Assistência Remota, com expressa anuência do usuário solicitante.

§ 5º A DSGTI e as CORTIs ficarão responsáveis unicamente pela manutenção dos RTI pertencentes ao Instituto, não prestando nenhum tipo de suporte a equipamentos de uso pessoal (notebooks, computadores, equipamentos de rede e etc.).

§ 6º Fica **TERMINANTEMENTE PROIBIDO** que qualquer servidor do IFAC, execute suporte técnico em equipamentos de uso particular, dentro do Instituto.

Art. 47 Os equipamentos de informática, disponibilizados nas diversas áreas, destinam-se, exclusivamente, à realização das atividades inerentes aos serviços desta instituição.

Art. 48 Aos usuários dos equipamentos de informática e comunicação de dados do IFAC é vedado instalar produtos e sistemas que não tenham sido homologados e adquiridos pela DSGTI e CORTIs.

Art. 49 Todos os equipamentos ligados à rede devem obedecer a padrões de instalação, de designação de endereços e domínio, portanto, uma vez aprovada a solicitação, será realizada a adição do equipamento pela DSGTI e CORTIs.

Art. 50 Na utilização dos RTIs do IFAC, o usuário deve, obrigatoriamente:

§ 1º Zelar pelos RTIs que utiliza, conservando suas características físicas ou componentes integrantes da rede;

§ 2º Não prejudicar deliberadamente o uso dos RTIs do IFAC seja por meio de software, de hardware ou ação direta na rede;

§ 3º Ao utilizar as facilidades da conexão com a Internet, fazê-lo de forma adequada, considerando que tal recurso está disponível ao usuário para fins acadêmicos, científicos e/ou administrativos;

§ 4º Não formatar qualquer equipamento do IFAC ou reinstalar seu sistema operacional sem autorização da DSGTI ou do setor local de suporte;

§ 5º Não remover ou modificar, de qualquer equipamento do IFAC, qualquer configuração do sistema operacional e/ou software responsável pela manutenção da integridade do próprio equipamento ou da rede, como firewall, acesso a domínio, antivírus, clientes de monitoramento e outros;

§ 6º Não adicionar à rede do IFAC quaisquer RTIs que possam interferir de alguma forma no desempenho ou na segurança da rede, como notebooks, pontos de acesso wireless, computadores novos, impressoras de rede, sem autorização da DSGTI em se tratando da reitoria ou pelas CORTIs nos campi;

§ 7º Caso autorizado o uso de RTIs particulares na rede institucional, obedecerão às normas estabelecidas por essa resolução e demais critérios normatizados e estipulados pelo CGSIC.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

§ 8º Não instalar, copiar e/ou utilizar softwares proprietários sem o devido licenciamento e autorização da DSGTI em se tratando da reitoria ou pelas CORTIs nos campi, em qualquer equipamento do IFAC;

§ 9º Não permitir acesso a qualquer RTI do IFAC por pessoas não autorizadas;

§ 10 Não criar ou propagar vírus, mensagens em massa (spams) e similares que venham danificar ou interferir de qualquer forma nos RTIs do IFAC ou externos à instituição;

§ 11 Não acessar de forma deliberada áreas em disco ou memória de qualquer RTI do IFAC, principalmente de máquinas servidoras de responsabilidade da DSGTI e campi, que sejam de acesso restrito;

§ 12 Não utilizar os RTIs para o monitoramento não autorizado de mensagens eletrônicas ou de quaisquer transmissões de dados;

§ 13 Não utilizar os RTIs em atividades particulares de forma que possa prejudicar suas atividades profissionais ou de outras pessoas da instituição ou lesar o patrimônio público, que possua fins lucrativos, ou seja, em benefício de organizações que não tenham relação com o IFAC;

§ 14 Não criar, transmitir, distribuir, disponibilizar e/ou armazenar documentos de qualquer espécie que não estejam de acordo com a lei ou regulamentações, notadamente àqueles referentes aos crimes informáticos, ética, decência, pornografia, honra e imagem de pessoas, organizações ou empresas, vida privada e intimidade;

§ 15 Não guardar ou retransmitir qualquer documento originalmente digital ou digitalizado a partir de documentos impressos a não ser que seja respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos no âmbito da Administração Pública Federal (Decreto nº4.553 de 27 de dezembro de 2002) e os direitos autorais (Lei nº 9.610, de 19 de fevereiro de 1998);

§ 16 Manter os gabinetes dos computadores fechados, sendo abertos somente com autorização da DSGTI na reitoria ou CORTIs nos campi;

§ 17 Não remover a etiqueta com o número do patrimônio, etiqueta da DSGTI e etiquetas do fabricante dos equipamentos, e, em caso de queda acidental da etiqueta comunicar imediatamente o Setor de Patrimônio.

§ 18 Não proceder à abertura de equipamentos para qualquer tipo de reparo, caso em que deverão ser solicitadas à DSGTI na reitoria ou CORTIs nos campi as devidas providências.

§ 19 Recomenda-se que o usuário desligue sua estação de trabalho ao final do seu expediente. Quando for necessário o processamento das estações de trabalho, fora do expediente normal, o usuário deve comunicar a sua necessidade a DSGTI na reitoria ou CORTIs nos campi.

Art. 51 O atendimento aos usuários do IFAC para qualquer serviço relacionado a RTIs, deverão estar de acordo com esta política.

Art. 52 A DSGTI na reitoria e CORTIs nos campi farão, periodicamente, cópia de segurança dos arquivos de seus computadores centrais (servidores de rede e de arquivos).

§ 1º Os usuários deverão proceder à avaliação dos arquivos armazenados nas estações de trabalho (drive local), visando à execução de cópia de segurança daqueles considerados importantes.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

§ 2º Os arquivos gerados nas estações de trabalho são de propriedade exclusiva do IFAC e serão armazenados, preferencialmente, no servidor de arquivos do Órgão.

§ 3º A DSGTI e CORTIs não se responsabilizarão por nenhum arquivo armazenado no disco local da estação de trabalho, sendo de responsabilidade de o usuário armazenar uma cópia de segurança de seus arquivos de trabalho na pasta compartilhada do servidor disponibilizado para este fim.

§ 4º Cada setor terá sua pasta no repositório de arquivos, e o seu conteúdo estará visível somente para os servidores daquele setor, sendo seu uso exclusivo para fins Institucionais, não sendo permitido o armazenamento de arquivos pessoais, cabendo se necessário Sanções Administrativas.

§ 5º O espaço em disco nos servidores que armazenam informações de usuários cadastrados poderá ser limitado por quotas individuais ou de grupos, de acordo com a disponibilidade técnica de cada máquina servidora e considerando o perfil de usuário e grupo. Quotas maiores poderão ser concedidas mediante solicitação com justificativa escrita e autorização da Reitoria ou das Direções das Unidades de Ensino.

§ 6º Poderá haver uma pasta de troca de arquivos entre setores, lembrando que os arquivos nesta pasta específica serão eliminados periodicamente e não serão feitas cópias de segurança dos mesmos.

CAPÍTULO VII DO USO DE IMPRESSORAS

Art. 53 Este capítulo define as normas de utilização de impressoras disponíveis nos departamentos da Instituição. Esta política é aplicada aos professores efetivos ou substitutos, alunos, servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço do IFAC que utilizam impressoras em seus departamentos, sendo que, nos laboratórios de ensino, que são utilizados pelos alunos, não existem impressoras instaladas.

§ 1º Antes de mandar imprimir, deve-se verificar se a impressora está ligada e abastecida de papel e, quando esta estiver ligada a um computador, se o mesmo também está ligado;

§ 2º A DSGTI poderá proceder com a instalação de um servidor de impressão que periodicamente emitirá relatórios de quantitativos impressos por usuário da rede.

I. Havendo impressora abastecida e em funcionamento no seu setor deve-se utilizá-la a fim de não onerar outro centro de custos;

II. Antes de mandar reimprimir, deve-se verificar se ainda não foi impresso;

III. Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro, impressões erradas ou inutilizadas devem ser utilizadas como rascunho ou armazenadas adequadamente para reciclagem.

IV. Se a impressora emitir alguma folha em branco, deve ser recolocada na impressora.

V. É responsabilidade de o usuário realimentar a gaveta de papéis sempre que estiver vazia ou no final.



VI. Impressora colorida só deve ser utilizada para versão final e com autorização da chefia imediata.

CAPÍTULO VIII

DO ACESSO E UTILIZAÇÃO DA INTERNET

Art. 54 Para obter uma conta de acesso à Internet para servidores e/ou usuários temporários, a chefia imediata ou o setor de Recursos Humanos deverá solicitar a DSGTI, por meio do sistema de abertura de chamado, informando:

- I.** Nome completo do usuário;
- II.** Setor no qual está desempenhando suas atividades;
- III.** Matrícula;
- IV.** Justificativa da necessidade da conta de acesso à Internet;

Parágrafo único. Para usuários temporários, a conta criada terá data e hora fixa de expiração.

Art. 55 Para obter uma conta de acesso para os alunos, o Registro Escolar de cada Campus emitirá uma relação de alunos matriculados com os seguintes dados necessários para o cadastro:

- I.** Nome completo;
- II.** CPF;
- III.** Data de nascimento;
- IV.** Matrícula;
- V.** Curso.

Art. 56 A DSGTI efetuará o cadastro e informará ao solicitante o usuário, senha padrão/provisória criados e dará conhecimento das normas de uso da Internet;

Art. 57 Para desativar uma conta de acesso o gestor imediato deverá solicitar a DSGTI por meio do sistema de abertura de chamados, informando:

- I.** Nome completo do usuário;
- II.** Setor no qual está desempenhando suas atividades;
- III.** Matrícula;
- IV.** Justificativa formal.

Parágrafo único Quando da mudança de setor ou desligamento, o gestor imediato deverá comunicar a DSGTI para que o remanejamento do usuário seja realizado.

Art. 58 A Internet Institucional é uma ferramenta de trabalho e deverá ser utilizado para fins acadêmicos, científicos e/ou administrativos do IFAC, não sendo permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

Art. 59 O acesso à Internet, no âmbito do Órgão, deve ser considerado como uma concessão e não um direito, portanto todos os usuários ao utilizarem este serviço, deverão fazê-lo no interesse da Instituição, mantendo uma conduta profissional, especialmente em se tratando de utilização de bem público.

Art. 60 O acesso à Internet é feito unicamente pela conexão provida pelo órgão, ficando proibida a utilização diferente desta.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 61 Todas as contas com perfil administrativo terão uma titularidade, determinando a responsabilidade sobre a sua utilização;

Art. 62 O acesso à Internet será monitorado por meio de ferramentas próprias, podendo os acessos serem auditados quando necessário. Todos os registros de acessos à Internet são passíveis de auditoria;

Art. 63 Todo o tráfego na rede é considerado confidencial, portanto, é proibida a divulgação e/ou compartilhamento de informações confidenciais em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

Art. 64 Somente usuários autorizados a falar, analisar ou publicar documentos em nome do IFAC poderão fazê-los em comunicações eletrônicas;

Art. 65 O IFAC mantém o direito de cópia de todo material postado na Internet por qualquer usuário no curso de suas obrigações;

Art. 66 Nenhum dos serviços de Internet do IFAC poderá ser utilizado para fins particulares.

Art. 67 É expressamente proibido o acesso à Internet para violar leis e regras brasileiras ou de qualquer outro país, como download, upload ou distribuição de conteúdos que ferem os direitos autorais e/ou licenças de uso. O uso dos recursos de Internet provido pelo IFAC para atividades ilegais é razão para perda de privilégios e ações administrativas e penais cabíveis;

Art. 68 A navegação a sites não relacionados diretamente à atividade administrativa ou acadêmica dos usuários não é proibida, respeitando o art. 3º IX, porém seu uso deve ser feito de maneira equilibrada e responsável, para assegurar ao usuário e ao Instituto máxima segurança e desempenho no trabalho, de modo que abusos serão punidos com bloqueio de acesso a tais sites sem prévio aviso.

Art. 69 São considerados usos indevidos, abusivos ou excessivos da Internet do IFAC: o racismo, terrorismo, hacker, assédio sexual e moral, pornografia, pedofilia, incentivo a violência, discriminação, como instrumento de ameaça, calúnia, injúria ou difamação e outros não condizentes com os objetivos de trabalho como:

§ 1º Acesso a portais não relacionados à atividade funcional ou às informações não necessárias à atualização e o desenvolvimento profissional;

§ 2º Acesso a sites de conversação (bate-papo, *webchat*);

§ 3º Sites de *proxy* e ferramentas que permitam o acesso anônimo;

§ 4º Jogos on-line e/ou de rede (*LAN*) de qualquer tipo, salvo com conteúdo relacionado diretamente à atividades administrativas e/ou educacionais;

§ 5º Programas que implementem P2P, onde o computador do usuário atua como servidor, como *Kazaa*, *Emule*, *Net-Meeting*, *Napster*, *Groove*, *ICQ*, *Morpheus*, *Bittorrent*, *Ares* e afins;

§ 6º *Web* rádio e *Web* TV (sessões de transmissão contínua de vídeo e áudio), a menos que estes sites estejam dentro do escopo de obrigações regulares;

§ 7º Baixar arquivos (*downloads*) de som (*mp3*) e vídeo que ferem os direitos autorais e/ou licenças de uso ou executar arquivos do tipo *exe*, *dat*, *sys*, *bat* e outros tipos de arquivos



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

executáveis, a menos que estes arquivos estejam dentro do escopo de obrigações regulares e/ou acadêmicas;

§ 8º Distribuir *software* ou conteúdo não autorizado (pirataria);

§ 9º Uso da rede para circulação de propaganda política;

§ 10 Disseminar vírus, *worms*, cavalos de troia ou qualquer outro tipo de código malicioso;

§ 11 Fazer download de programas não relacionados às atividades fins e acessórias do IFAC;

§ 12 Adotar de forma independente da DSGTI, quaisquer mecanismos de codificação /criptografia;

Art. 70 Caso a DSGTI ou as CORTIs julguem necessário, haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, ou desempenho e produtividade das atividades dos usuários, bem como, que exponham a rede a riscos de segurança.

Art. 71 Serão bloqueados sites de pornografia, pedofilia e outros contrários a legislação em vigor e as definições desta Política.

Art. 72 É obrigatória a utilização do (s) *software(s)* homologado (s) pela DSGTI tais como *Mozilla Firefox, Internet Explorer, Google Chrome* como cliente (s) de navegação;

Art. 73 O acesso a sites de relacionamentos, poderão ser bloqueados de acordo com a necessidade da Instituição.

CAPÍTULO IX DA PUBLICAÇÃO NA INTERNET

Art. 74 A criação de páginas e perfis nas mídias sociais, bem como sistema com a marca “IFAC” será feita mediante a apresentação de projeto à DSCOM para análise e devida aprovação, com antecedência.

Parágrafo único. Considerando que as páginas próprias são documentos públicos disponíveis para qualquer pessoa em qualquer lugar e que o domínio “ifac.edu.br”, ao qual tais páginas pertencem, é um bem intangível importante do IFAC, a Reitoria se reserva o direito de avaliar seu conteúdo, permitindo ou não sua publicação, já que tais documentos podem influenciar na formação da imagem da instituição e na sua reputação frente à comunidade.

Art. 75 É terminantemente proibida a publicação de páginas com os seguintes conteúdos ou *links*:

- I. De cunho puramente pessoal, sem vinculação com suas atividades na instituição;
- III. Comerciais ou de caráter publicitário;
- IV. De caráter político-partidário ou religioso;
- V. Caluniosos, difamatórios ou ameaçadores;
- VI. Que infrinjam a legislação sobre direitos autorais e propriedade intelectual;
- VII. Ofensivos ou que façam uso de linguagem ofensiva;
- VIII. Que incite a qualquer tipo de discriminação;
- IX. Que incitem à violência;
- X. Pornográfico de qualquer natureza;



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

XI. Com imagens ou dados que possam ser considerados abusivos, profanos, incômodos.

Parágrafo único. Eventuais ocorrências não previstas neste artigo serão analisadas pelos órgãos competentes do IFAC.

Art. 76 A Diretoria Sistêmica de Comunicação – DSCOM é responsável pela divulgação de informações na página principal da instituição.

§ 1º Outros setores da instituição poderão ter acesso à administração de determinados itens da página principal do IFAC para publicação de documentos oficiais e notícias da instituição de sua responsabilidade.

§ 2º A DSGTI é responsável pela permissão de acesso às áreas de administração da página principal do IFAC aos usuários que forem designados pela Reitoria.

Art. 77 A DSCOM é responsável pela divulgação de informações e disponibilização de material na Intranet do IFAC, *website* de uso interno que só poderá ser acessado por usuários cadastrados.

Parágrafo único. A DSCOM poderá delegar poderes a outros usuários para a divulgação de informações na Intranet, concedendo acesso, ficando este usuário responsável pelas informações.

Art. 78 Outros domínios e/ou subdomínios de Internet, hospedados em máquinas servidoras do IFAC ou não, poderão ser instalados no ambiente de rede do IFAC, desde que sejam de interesse da instituição e não infrinjam nenhum dos artigos desta resolução, tendo que ser, portanto, autorizados previamente pela Reitoria.

Art. 79 O IFAC não se responsabilizará por publicações realizadas fora do domínio “ifac.edu.br”.

CAPÍTULO X DAS RESPONSABILIDADES

Seção I Dos usuários

Art. 80 Se algum usuário souber de qualquer violação a esta Política deverá comunicar imediatamente a DSGTI, CGSIC ou a sua chefia imediata.

Art. 81 Evitar utilizar a Internet, para a prática de atos ilícitos, proibidos pela lei ou pela presente política, como também danificar e/ou sobrecarregar os recursos tecnológicos (hardware e software);

Art. 82 Quando preencher um formulário ou enviar informações confidenciais por meio da Internet certificar-se que a conexão está segura através do símbolo do cadeado fechado (SSL) que aparece no canto inferior direito do browser e da palavra HTTPS substituindo a palavra HTTP na barra de endereço do browser, para certificar que os dados estão sendo enviados de forma segura pela Internet;

Art. 83 Desconectar-se imediatamente de um site que contenha acesso restrito, mesmo que tenha sido aceito pelos sistemas encarregados de barrá-lo.

Art. 84 Evitar advogar causas políticas e de emitir informações não autorizadas sobre quaisquer serviços, produtos, contextos políticos, dentre outros na Internet.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 85 O usuário é o responsável pelos acessos à Internet realizados pela sua conta.
§ 1º O mau uso de uma conta de acesso à Internet por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis.
§ 2º O usuário deverá zelar pelo fiel cumprimento ao estabelecido nesta Política.

Seção II
Da DSGTI

Art. 86 Implantar apenas um ponto de conexão à Internet, para que todos os usuários se autenticuem neste ponto.

Art. 87 Implantar mecanismos de monitoramento dos acessos à Internet.

Art. 88 Arquivar todas as solicitações de acesso à Internet para controle.

Art. 89 Adotar mecanismos de criptografia/codificação para transferência de informações sensíveis pela Internet.

Art. 90 Verificar periodicamente os acessos à Internet, para detectar eventuais problemas que possam estar ocorrendo.

Art. 91 Fornecer quando solicitado pelo Gabinete, relatório de acessos dos usuários.

Art. 92 Definir e homologar browser (navegador) a ser utilizado e prover mecanismos de atualizações e correções de segurança.

Art. 93 Bloquear sites que vão de encontro a esta Política e que estejam comprometendo o bom funcionamento dos recursos de Internet.

Art. 94 Cabe a DSGTI na reitoria gerir e monitorar a infraestrutura de equipamentos (hardware) e aplicativos (software) necessária à prestação dos serviços de acesso a redes externas e à Intranet, assim como nos campi caberá às CORTIs.

Art. 95 A DSGTI e CORTIs poderá efetuar à desinstalação sumária dos produtos que não se enquadrarem nos critérios estabelecidos por essa Resolução.

CAPÍTULO XI
DA SEGURANÇA FÍSICA

Art. 96 O objetivo desta política é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da Instituição. A segurança física dos equipamentos de informática e das informações da Instituição deve ser protegida de possíveis danos. Será abordada a segurança física dos laboratórios de informática, das instalações de TI, dos equipamentos no geral e procedimentos para garantir a segurança.

Seção I
Controle de acesso

Art. 97 Existem áreas que merecem maior atenção quanto ao controle da entrada de pessoas, estas áreas são departamentos que contém informações ou equipamentos que devem ser protegidos, como por exemplo: Área de TI, sala de servidores, departamento financeiro,



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

setor de documentação, departamento de recursos humanos, sala de coordenadores e diretores, entre outras.

§ 1º Apenas pessoas autorizadas podem acessar as instalações de TI da DSGTI na reitoria e nos campi deverá estar autorizada pelas CORTIs.

§ 2º Aos departamentos que tratam informações confidenciais de alunos como, por exemplo, documentação, informações financeiras e acadêmicas, o acesso deve ser permitido somente para pessoas autorizadas.

§ 3º A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

§ 4º Se acontecer a perda de chaves de departamentos ou laboratórios, a coordenação responsável deve ser informada imediatamente para que possa providenciar a troca da fechadura e de outras cópias da chave perdida.

CAPÍTULO XII

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS

Art. 98 Este capítulo normatiza a política de cópias de segurança (backup) e restauração de dados corporativos armazenados no parque tecnológico do IFAC.

Art. 99 Abrange os dados corporativos existentes nos servidores de rede.

Art. 100 As diretrizes deste documento deverão ser aplicadas em todos os Campi que compõem o IFAC, bem como na Reitoria.

Seção I

Das definições

Art. 101 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*;



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

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

Seção II
Diretrizes gerais

Art. 102 Cabe aos administradores da rede, analistas de TI, técnicos de TI e gestores da instituição em conjunto com CGSIC:

- § 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;
- § 10 Prover os recursos necessários para implantar a política de backup;
- § 11 Planejar e executar a realização de testes periódicos de restauração dos backups;
- § 12 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;
- § 13 As mídias (ou dispositivos de armazenamento) deverão ser armazenados em locais seguros, de preferência em localidade diversa da origem dos dados (backup off-site);
- § 14 As solicitações de restauração de arquivos deverão ser abertas formalmente através de ferramentas de abertura de chamados e deverão conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso;
- § 15 O proprietário dos dados deverá ter ciência dos tempos de retenção aqui estabelecidos para cada tipo de informação;
- § 16 Os administradores/operadores de backup deverão zelar pelo cumprimento das diretrizes aqui estabelecidas.

Seção III
Backup dos dados nas estações de trabalho

Art. 103 O *backup* dos arquivos pessoais existentes nas estações de trabalho é de inteira responsabilidade dos usuários, que deverão fazê-lo em mídia própria;



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 104 Os dados corporativos criados ou mantidos pelos usuários deverão ser armazenados em local próprio indicado pela Coordenação de TI dos respectivos campi e pela DSGTI na reitoria.

Art. 105 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 setor;

Art. 106 A DSGTI e as CORTIs dos campi não se responsabilizarão pela integridade dos backups feitos pelos usuários em qualquer mídia de armazenamento;

Art. 107 A DSGTI e as CORTIs dos campi não se responsabilizarão pela perda dos dados corporativos armazenados nas estações de trabalho ou em quaisquer mídias de armazenamento não indicadas.

Seção IV

Backup dos dados corporativos

Art. 108 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 *Wi-fi* 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



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

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.

Seção V
Recuperação de dados

Art. 109 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.

Seção VI
Teste de recuperação de dados

Art. 110 A recuperação de dados será realizada mediante solicitação via sistema de abertura de chamado 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.

CAPÍTULO XIII
DA UTILIZAÇÃO DE LABORATÓRIOS DE INFORMÁTICA

Seção I
Orientações gerais

Art. 111 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.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 112 Para utilização de laboratórios e equipamentos de informática algumas regras devem ser cumpridas para que possa ser feito uso correto das instalações evitando qualquer tipo de dano a equipamentos em laboratórios que possam prejudicar a utilização dos mesmos.

§ 1º O acesso a laboratórios de informática deve ser controlado, somente sendo permitido o uso dos mesmos com um professor, servidor e/ou monitor responsável.

§ 2º É de responsabilidade do professor, servidor e/ou monitor que utilizou o laboratório zelar pela ordem das instalações. Sendo necessário qualquer tipo de manutenção, a DSGTI ou a equipe local de suporte deve ser informada.

§ 3º No momento em que entrar no laboratório o professor, servidor e/ou monitor responsável deve verificar se todos os computadores estão funcionando corretamente. Após a utilização esta verificação deve ser repetida, e qualquer problema a DSGTI ou a equipe local de suporte deve ser informada, para que a solução possa ser providenciada o mais rápido possível.

§ 4º Os equipamentos devem ser trancados e em segurança quando deixados sem supervisão, não sendo permitida a utilização de laboratórios sem supervisão.

§ 5º Nenhum equipamento pode ser conectado aos sistemas ou rede sem aprovação prévia e, se necessário, sob supervisão.

§ 7º As chaves de acesso aos laboratórios devem ficar guardadas em locais que o acesso seja controlado, que não seja permitida a entrada de pessoas não autorizadas, evitando que possam ter acesso às chaves.

§ 8º Se a utilização do laboratório não estiver prevista no horário, essa utilização deverá ser feita somente mediante a reserva do laboratório, garantindo assim que exista um registro de utilização dos mesmos.

Art. 113 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. 114 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. 115 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. 116 Qualquer problema nos equipamentos deve ser reportado ao técnico do laboratório ou ao Setor de tecnologia da informação, via Sistema de abertura de chamado, para que este seja solucionado.

Art. 117 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.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Art. 118 Os usuários dos laboratórios comprometem-se a utilizar os recursos exclusivamente para atividades de ensino, pesquisa e extensão.

Art. 119 Os usuários só terão acesso aos laboratórios nos horários previstos para aulas ou em casos excepcionais com autorização do Departamento de Ensino.

Art. 120 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. 121 É proibido nos Laboratórios:

- I.** Remover ou Danificar equipamentos e periféricos (mouse, teclado, monitor de vídeo, entre outros.);
- II.** Gravar *CDs* e *DVDs*, salvo com consentimento do professor, técnico responsável ou Setor de tecnologia da informação;
- III.** Trazer ou retirar mesas e cadeiras sem prévia autorização do Departamento de Ensino ou do Patrimônio;
- IV.** Desenvolver, disseminar ou utilizar programas que tenham objetivo de obter senhas, informações pessoais de outros usuários ou acessar informações restritas;
- V.** Utilização de jogos para fins não educacionais;
- VI.** Acessar páginas ou utilizar software com conteúdo pornográfico;
- VII.** Fumar e/ou consumir qualquer tipo de alimento ou bebidas;
- VIII.** 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. 122 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. 123 Caso o usuário tenha dúvida a respeito de realizar alguma atividade, deve consultar o Departamento de Ensino ou Setor de tecnologia da informação.

Art. 124 Algumas recomendações que constituem boas práticas de utilização dos laboratórios:

- I.** Os computadores devem ser desligados no final da seção diária de trabalho pelos próprios usuários;
- II.** Arquivos gravados, pelo usuário, em discos rígidos devem ser copiados para seu dispositivo de armazenamento pessoal ao terminar a sessão diária de uso;
- III.** Problemas e ocorrências estranhas observadas com o equipamento devem ser reportados ao professor ou Setor de tecnologia da informação, conforme o caso;
- IV.** As cadeiras devem ser reorganizadas após o uso dos laboratórios.

Art. 125 Os alunos, no ato da matrícula, assinarão um termo de compromisso, comprometendo-se a seguir as Políticas de Segurança e dando ciência das normas estabelecidas.



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

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. 126 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.

CAPÍTULO XIV
SANÇÕES ADMINISTRATIVAS

Art. 127 Para fins desta política serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

- I.** Na Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;
- II.** No Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;
- III.** No Código Penal, através do Decreto-Lei nº 2848/1940;
- IV.** Na Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;
- V.** No Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- VI.** Na resolução 161/2013 que dispõe sobre o Regimento Disciplinar Discente.

Art. 128 Em todo caso, deverão ser assegurados o contraditório e a ampla defesa, conforme consagrados na Constituição da República Federativa do Brasil de 1988.

Art. 129 Reserva-se o direito a DSGTI 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 implicará na aplicação de sanções administrativas, cíveis e penais de acordo com a legislação vigente ou em qualquer outra legislação que regule ou venha regular a matéria.

Art. 130 Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, a violação pode ter ocorrido por negligência, acidente, erro ou por ação previamente determinada, ignorando a política estabelecida.

Art. 131 Técnicos da DSGTI identificarão os usuários - doravante chamados de infratores - que violarem qualquer item desta política de segurança.

Art. 132 O não cumprimento, pelo servidor, terceirizados e/ou estagiários das normas estabelecidas neste documento seja isolada ou cumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: Comunicação de Descumprimento, Advertência ou Suspensão.

§ 1º Na primeira transgressão, esses infratores serão notificados, via e-mail, do descumprimento das Normas estabelecidas neste documento;



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Acre

§ 2º Caso haja uma segunda transgressão da política, num período de 90 dias, esses infratores serão novamente notificados, via e-mail, sendo que uma cópia da notificação será enviada para o gestor superior da área e para o Diretor de Campus.

§ 3º Comunicação de Descumprimento: Será encaminhado ao servidor, por e-mail, comunicado informando o descumprimento da política, com a indicação precisa da violação praticada.

§ 4º Advertência ou Suspensão: Na terceira transgressão, será aplicado por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.

§ 5º Todos os comunicados de descumprimento desta política permanecerão arquivados junto a Diretora Sistêmica de Gestão de Pessoas na respectiva pasta do servidor.

§ 6º Caso seja necessário advertir o aluno, será informada a Coordenação do Curso a qual o aluno está matriculado para interagir e manter-se informado da situação.

§ 7º Cabe a Coordenação de Curso, emitir comunicado informando o descumprimento da política pelo aluno, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a respectiva pasta do aluno.

§ 8º A pena de advertência ou suspensão será aplicada, na hipótese de reincidência na prática de infrações. Antes da aplicação desta punição será realizado o conselho de disciplina, conforme regimento escolar que detalha os direitos e deveres dos alunos.

Art. 133 Os casos omissos serão dirimidos pelo Comitê Gestor de Segurança da Informação e Comunicações – CGSIC.