MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ

INSTRUÇÃO NORMATIVA N° 01/2023 - CIGD

Institui as Políticas de Privacidade, Controle de Acesso e Uso de Recursos de TIC da Universidade Federal do Paraná

O Comitê Institucional de Governança Digital da Universidade Federal do Paraná, no uso de suas atribuições e, considerando:

1) Os artigos 46, 47 e 50 da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais);
2) A Resolução 38/22-COPLAD, que estabelece a Política de Segurança da Informação da UFPR;

Resolve:

Art. 1º - Instituir as Políticas de Privacidade, de Controle de Acesso e de Uso de Recursos de Tecnologia da Informação e Comunicação da Universidade Federal do Paraná, na forma de anexos dessa Instrução Normativa.

Art. 2º - Essa instrução Normativa entra em vigor na data de sua publicação.

ANEXO I
POLÍTICA DE PRIVACIDADE

A Lei 13709/2018 - Lei Geral de Proteção de Dados (LGPD) estabelece como fundamento o respeito à privacidade. Desse modo, a presente Política de Privacidade ("Política") tem o propósito de comunicar de forma simples quais tipos de dados pessoais serão coletados, quando, de que forma e para quais finalidades serão utilizados. Demonstra-se que a privacidade de todos os integrantes da nossa comunidade à qual servimos, como estudantes, servidores, funcionários terceirizados e cidadãos ("você", "titular"), é importante para a UNIVERSIDADE FEDERAL DO PARANÁ ("UFPR") e, por esta razão, empenhamos os maiores esforços para proteger os dados pessoais que tratamos.

A Política se aplica a quaisquer atividades da UFPR, consequentemente, compreendem todas as suas atuações, sejam elas acadêmicas, como Ensino, Pesquisa e Extensão, ou administrativas.

Dados pessoais são considerados quaisquer dados relacionados a uma pessoa natural identificada ou identificável, dados de localização ou identificadores eletrônicos, sempre que estiverem relacionados a uma pessoa, ou seja, qualquer informação pessoal que possa identificar o seu titular.

1. **Das Informações Gerais**
    1. **Dos dados da UNIVERSIDADE FEDERAL DO PARANÁ**

UNIVERSIDADE FEDERAL DO PARANÁ, pessoa jurídica de direito público, inscrita no CNPJ/ME sob nº 75.095.679/0001-49 com sede na Rua XV de Novembro, 1299, Cidade de Curitiba, Estado do Paraná, CEP 80.060-000, doravante simplesmente "UFPR".

2. **Do Encarregado de Proteção de Dados Pessoais**

Em consonância com o Art. 41 da LGPD, o Encarregado de Proteção de Dados Pessoais (DPO) na UFPR foi nomeado pela Portaria 549/reitoria, de 22/07/21:

Prof. Luis Fernando Lopes Pereira – Telefones (41) 3310-2610 ou 3310-2611
sic@ufpr.br
Prédio Histórico – Praça Santos Andrade, 50
Andar Térreo (Acesso pela Rua XV de Novembro)
Curitiba – PR – CEP 80020-300

3. **Dos termos e definições**

i. **Autoridade Nacional de Proteção de Dados (ANPD):** agência reguladora da Lei Geral de Proteção de Dados Pessoais – LGPD.
ii. ***Cookies***: Um pequeno arquivo que é salvo no computador das pessoas para ajudar a armazenar as preferências e outras informações usadas nas páginas da Web que elas visitam.
iii. **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. À luz da LGPD, o controlador é a UFPR.
iv. **Dado pessoal:** É qualquer informação relacionada a pessoa natural identificada ou identificável.
v. **Dado pessoal sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
vi. **Encarregado de Proteção de Dados Pessoais:** Pessoa indicada pela UFPR para atuar como canal de comunicação entre o controlador, os

titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Ver item 1.2.

vii. **Lei Geral de Proteção de Dados (LGPD):** é a lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que (i) a operação de tratamento seja realizada no território nacional; (ii) a atividade de tratamento que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

viii. **Operação de dados pessoais:** o mesmo que tratamento de dados pessoais, toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

ix. **Operadores:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. No caso da UFPR, são as fundações de apoio – FUNPAR (Fundação da Universidade Federal do Paraná) e FUPEF (Fundação de Pesquisas Florestais do Paraná), o Complexo Hospital de Clínicas e empresas terceirizadas que nos prestam serviços.

x. **Política de Segurança da Informação e Comunicação (POSIC):** documento no qual a UFPR assume o compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda/custódia, devendo ser cumprida por todos os seus colaboradores e operadores. Seu propósito é estabelecer as diretrizes a serem seguidas pela UFPR e os operadores no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

xi. **Titular/ titular dos dados:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

2. Dos dados coletados

Os dados que tratados pela UFPR são utilizados unicamente para atendimento à comunidade, para cumprimento de obrigações legais ou regulatórias, para execução, acompanhamento ou monitoramento de políticas públicas, ou ainda para fins de pesquisa interna. Os dados poderão ser compartilhados com terceiros sempre com a base legal, de acordo com a LGPD e poderão ser anonimizados sempre que possível.

1. Da categorização dos titulares

i. **Alunos**, seja em cursos de ensino médio, pós-médio, graduação, pós-graduação *lato sensu* e *stricto sensu*, residência médica e multiprofissional ou de extensão;
ii. **Servidores** docentes e técnico-administrativos, ativos ou aposentados;
iii. **Terceiros**, que podem envolver terceirizados contratados, estagiários, conselheiros externos, ou qualquer cidadão da comunidade externa em geral;

2. Dos dados tratados

Os dados são coletados através de formulários específicos para cada finalidade, em websites ou formulários físicos, e servirão para finalidades específicas, em consonância com a LGPD e demais bases legais necessárias, conforme descrito na tabela a seguir.

Tipo de Dados		Dados Tratados	Aplicável a	Finalidade	Bases Legais
Dados Pessoais	Cadastrais e Acadêmicos	- Nome completo; - Documentos de identificação: RG, CPF, CTPS, CNPJ (MEI), Passaporte, PIS, título de eleitor, certificado militar, registro profissional de classe; - Sexo; - Estado civil; - Filiação; - Dependentes; - Nacionalidade; - Naturalidade; - Data, município e UF de nascimento; - País de origem; - Grau de instrução; - Tipo de escola que cursou o Ensino Médio; - Endereço, e-mail e telefone; - Diplomas e certificados; - Foto ou imagem pessoal - Instrumentos avaliativos; - Histórico escolar; - Currículo Lattes;	- Alunos; - Servidores; - Terceiros	- Cumprir sua missão educacional; - Cumprir obrigação legal, compartilhando autoridades e órgãos governamentais, quando requisitado e necessário; - Envio de atualizações, comunicados institucionais e/ou acadêmicas; - Histórico escolar e acervo acadêmico; - Emissão de declarações acadêmicas, Certidões, Histórico Escolar, Ementa, Diploma, Certificado e Certidões; Censo Universitário; Enade – Exame Nacional de Desempenho dos Estudantes; - Produção de carteiras de estudantes, crachá de servidores ou registros funcionais; - Identificação para acesso a Restaurantes Universitários;	- Art. 7º, inciso II - para o cumprimento de obrigação legal ou regulatória pelo controlador; - Art. 7º, inciso III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; - Art. 7º, inciso IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; - Art. 7º, inciso V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; - Art. 7º, inciso IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
	Dados de Gestão de Segurança da Informação	- Endereço IP; - Acessos; - Login;	- Alunos; - Servidores; - Terceiros	- Gestão e proteção da segurança da informação; - Cumprimento de mandados judiciais;	- Art. 7º, inciso II - para o cumprimento de obrigação legal ou regulatória pelo controlador; - Marco civil da internet

Tipo de Dados		Dados Tratados	Aplicável a	Finalidade	Bases Legais
	Financeiros	- Nome/número do banco; - Número de conta corrente/poupança; - Número da agência bancária; - Salário/remuneração; - Declaração de bens e renda; - Estágio externo à UFPR, remunerado ou não; - Ocupação profissional; - Recebimento de auxílios e bolsas dentro da instituição ou no âmbito de programas de inclusão social dos governos federal, estadual e municial; - Declaração financeiro de plano de saúde de titular e dependentes;	- Alunos; - Servidores; - Terceiros	- Pagamento de salário, remuneração ou bolsas; - Cumprimento de obrigações legais relativas à Lei da Transparência, quando couber; -Cumprimento da legislação trabalhista, tributária e previdenciária. Ainda normativa pertinente aos deveres de fiscalização de retenção de tributos de natureza fiscal e previdenciária. - Prestação de contas do auxílio per capta;	- Art. 7º, inciso II - para o cumprimento de obrigação legal ou regulatória pelo controlador; - Art. 7º, inciso III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; - Art. 7º, inciso IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; - Art. 7º, inciso V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; - Art. 7º, inciso IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; - Lei 8112/90, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.
		- Nome social; - Gênero; - Orientação sexual; - Cor/raça; - Tipo de deficiência; - Afiliação em sindicatos ou partidos políticos	- Alunos; - Servidores;	- Cumprir, monitorar e planejar a execução de políticas públicas; - Lançamentos de descontos sindicais em folha de pagamento; - Afastamento de servidor para exercício de mandato sindical, político ou participação em eleições;	- Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: - Art. 11, inciso II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para :a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; - Os princípios fundamentais da Constituição Federal (1988), postos em seu Art.3, que prima pela construção de uma sociedade livre, justa e solidária, que promove o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação, reduzindo as desigualdades sociais e regionais; - A Lei nº 9.394/1996, que ao tratar do princípios da educação em seu Art. 3, adverte que o ensino deve considerar da diversidade étnico-racial (Incluído pela Lei nº 12.796, de 2013) e a garantia do direito à educação e à aprendizagem ao longo da vida.(Incluído pela Lei nº 13.632, de 2018); - A Resolução nº 37/2004-COUN, que alterada pelas Resoluções nº 41/04-COUN e 17/07-COUN, que estabelece e aprova o Plano de Metas de Inclusão Racial e Social na Universidade Federal do Paraná; - A Lei nº 11.340/2006, que cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e

Tipo de Dados		Dados Tratados	Aplicável a	Finalidade	Bases Legais
Dados Pessoais Sensíveis	Cadastrais				Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal; e dá outras providências; - A Resolução 70/2008, que rege sobre o aprimoramento das políticas de ingresso e de permanência de pessoas com deficiências na Universidade Federal do Paraná; - A Declaração das Nações Unidas sobre os Direitos dos Povos Indígenas de 2008; - A Lei nº 12.288/2010, institui o Estatuto da Igualdade Racial, destinado a garantir à população negra a efetivação da igualdade de oportunidades, a defesa dos direitos étnicos individuais, coletivos e difusos e o combate à discriminação e às demais formas de intolerância étnica - A Lei Federal nº 12.711/2012, que dispõe sobre o ingresso nas universidades federais e nas instituições federais de ensino técnico de nível médio e dá outras providências; - A Lei n 13005/2014 – PNE, que em seu Art. 8o aponta para diretrizes metas e estratégias que considerem as necessidades específicas das populações do campo e das comunidades indígenas e quilombolas, asseguradas a equidade educacional e a diversidade cultural e garantam o atendimento das necessidades específicas na educação especial, assegurado o sistema educacional inclusivo em todos os níveis, etapas e modalidades; - A Lei nº 13.146/2015 – Lei Brasileira de Inclusão da Pessoa com Deficiência, que eu seu Art. 3º aponta em seu Inciso III, a necessidade de garantir a tecnologia assistiva ou ajuda técnica: produtos, equipamentos, dispositivos, recursos, metodologias, estratégias, práticas e serviços que objetivem promover a funcionalidade, relacionada à atividade e à participação da pessoa com deficiência ou com mobilidade reduzida, visando à sua autonomia, independência, qualidade de vida e inclusão social; - A Lei nº 13.409/2016, que dispõe o ingresso sobre a reserva de vagas para pessoas com deficiência nos cursos técnicos de nível médio e superior das instituições federais de ensino; - A Lei no 13.445/2017, que trata da Lei de Migrações no Brasil; - A Resolução nº 33/17-COPLAD, que cria a Superintendência de Inclusão, Políticas Afirmativas e Diversidade (SIPAD) da Universidade Federal do Paraná e a aprovação por unanimidade do Processo: 042641/2019-81 que trata da Proposta do Regimento da Superintendência de Inclusão, Políticas Afirmativas e Diversidade adaptado ao SIORG, conforme consta na Ata da Sessão Extraordinária do Conselho de Planejamento e Administração da 2 Universidade Federal do Paraná realizada em 28 de junho de 2019; - Os princípios do Plano de Desenvolvimento Institucional 2017–2021, da Universidade Federal do Paraná. - Lei 8112/90, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. - Decreto 8727/2016, que dispõe sobre o uso do nome social e o reconhecimento da identidade de gênero de pessoas travestis e transexuais no âmbito da administração pública federal direta, autárquica e fundacional.

Tipo de Dados		Dados Tratados	Aplicável a	Finalidade	Bases Legais
	Saúde	- CIDs; - Exames; - Prontuário Médico; - Atestados médicos;	- Alunos e dependentes; - Servidores e dependentes; - Comunidade em geral;	- Atendimento aos programas de Saúde do Servidor; - Atendimento a alunos e familiares de servidores pelos programas da PROGEPE/UCSS; - Atendimento psicossocial a alunos; - Justificar ausências no sistema de frequência de servidores; - Exame admissional;	- Art. 11, inciso II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; - Art. 17, Lei nº 7.923/1989; - Decreto 67326/1970, que institui o SIPEC; - Os princípios do Plano de Desenvolvimento Institucional 2017–2021, da Universidade Federal do Paraná.
	Biométricos	- Imagem e voz através de aulas e atividades didáticas[1] ou administrativas realizadas através de forma remota[2]; - Imagem gravada através de câmeras de segurança;	- Alunos; - Servidores; - Terceiros	- Interação aluno/professor através de AVA's; - Disponibilização de conteúdo ministrado pelo docente em disciplinas remotas ou semi-presenciais; - Realização de bancas, palestras, workshops, *live streaming*, etc.; - Garantir a segurança de patrimônio público, estudantes, docentes e público em geral;	- Art. 11, inciso II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; e) proteção da vida ou da incolumidade física do titular ou de terceiro; - Art. 4, III, 'a' e 'd' – segurança pública e/ou atividades de investigação e repressão de infrações penais;

[1] Para aulas e atividades didáticas, acesse o Guia de Boas Práticas em https://lgpd.ufpr.br/portal/wp-content/uploads/2021/07/guia-de-boa-praticas.pdf

[2] Aulas presenciais somente poderão ser gravadas mediante consentimento explícito dos envolvidos, segundo RN 04/19-COUN, Art. 3º.

3. Atualização e veracidade dos dados

i. O titular e/ou seus responsáveis legais são os responsáveis pela atualização, exatidão e veracidade dos dados que informarem à UFPR.
ii. Caso sejam identificados erros de informações cadastradas, a UFPR solicitará ao Titular esclarecimentos e/ou correções;
iii. A UFPR não se responsabiliza por dados desatualizados em suas bases de dados, bem como pelo uso, pelo titular, dos ambientes da UFPR para quaisquer fins ilegais, ilícitos ou contrários à moralidade.

4. Base de Dados

i. O Titular dos dados declara estar ciente de que a base de dados formada por meio da coleta de dados nos sistemas da UFPR é de propriedade e de responsabilidade da UFPR e o seu uso será feito dentro das limitações desta Política e demais normas vigentes.
ii. A UFPR não irá vender, alugar ou emprestar os dados pessoais dos Titulares.
iii. A UFPR compartilha ou transfere dados dos titulares apenas nas hipóteses previstas nos itens 3.1 e 3.2.
iv. A UFPR e os operadores de dados pessoais que atuam em seu nome determinam que somente os empregados, servidores, estagiários e bolsistas devidamente autorizados terão acesso aos dados pessoais coletados e sempre respeitando os princípios de proteção e privacidade de dados, além da formalização de um compromisso de confidencialidade nos termos desta Política de Privacidade.

5. Cookies

A UFPR utiliza *cookies* de sessão para validação de acesso aos seus sistemas internos. Ao navegar pelos nossos *websites*, poderá haver uso de *cookies* de sessão, persistentes, de login e de comentários. Quando utilizados, será exibido um aviso ao usuário ao navegar pelo site.
Além dos cookies de sessão a UFPR pode, em determinados sites ou serviços, utilizar mecanismos de *trackers* para a análise de público onde será permitido ao usuário o aceite ou não do mesmo durante a navegação.

3. Do Compartilhamento de dados

1. Dados Compartilhados com Terceiros

Os dados que coletamos podem ser compartilhados com entidades terceiras quando necessário, e limitados estritamente aos dados suficientes para atendimento das seguintes hipóteses:

Compartilhado com	Tipo de Titular	Finalidade	Base Legal
Órgãos governamentais e de controle, autarquias	Alunos Servidores Terceirizados	Cumprimento de determinações ou obrigações legais, requerimentos ou requisições de órgãos governamentais ou ordens judiciais, fiscalização de conselhos profissionais;	Art. 7, incisos: - II: para o cumprimento de obrigação legal ou regulatória pelo controlador; - III: pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
Complexo Hospital de Clínicas	Servidores	Cumprimento de obrigações legais e tratativas relacionadas a vínculo funcional;	
Fundações de Apoio	Alunos Servidores	Quando da participação do titular em convênios, para pagamento de bolsas e prestação de contas	
Prestadores de serviço	Alunos Servidores Terceirizados	Atendimento à prestação de serviços necessários para ferramentas de trabalho ou execução de atividades acadêmicas, como servidores de e-mail, aplicativos de terceiros, armazenamento de arquivos, etc;	
Comunidade acadêmica interna ou externa	Alunos Servidores	Disponibilização de aulas gravadas com intuito exclusivamente educacional;	- Art. 11, inciso II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
Universidades nacionais	Alunos	Mobilidade acadêmica	Art. 7, - III: pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

2. Transferência Internacional

A Agência Internacional da UFPR compartilhará os dados do histórico escolar e de identificação do passaporte dos alunos que optarem por um dos programas vigentes de mobilidade, com a instituição acadêmica selecionada, com aquelas em que a UFPR possuir acordos vigentes.

Poderão ser compartilhados bancos de dados de pesquisa com universidades, agências de pesquisa ou semelhantes, sempre de maneira anonimizada.

Para atendimento à prestação de serviços necessários para ferramentas de trabalho ou execução de atividades acadêmicas, poderão ser contratadas empresas estrangeiras, ou empresas nacionais que farão uso de serviços estrangeiros para armazenamento de dados. Nestes casos, os operadores contratados respeitarão as políticas de proteção de dados definidas pela UFPR.

4. Do Prazo e da Forma de Armazenamento

i. Os dados serão armazenados para viabilidade dos serviços prestados pela UFPR, garantia dos direitos e cumprimento da Legislação Educacional, às atividades acadêmicas de acordo com os prazos de preservação documental estabelecidos pelo Ministério da Educação (Portaria MEC 1224/2013);
ii. Os dados digitais coletados serão armazenados em servidores de banco de dados geridos pela UFPR, utilizando as melhores práticas e tecnologias de segurança da informação aplicáveis;
iii. Os documentos físicos deverão ser armazenados em meios que garantam a proteção e restrição de acesso, sendo estas de responsabilidade da unidade que realiza a atividade de tratamento correspondente a tais documentos.
iv. Os dados de *cookies* de que trata o item 2.5 serão armazenados por até 6 meses do último acesso, conforme o Art. 15 do Marco Civil da Internet.

5. Dos Direitos dos Titulares

1. Quais são seus direitos

Os titulares têm direito à requisição gratuita de atendimento para:
i. Confirmar a existência de tratamento dos seus dados;
ii. Acessar os seus dados;
iii. Corrigir os seus dados que estejam incompletos, inexatos ou desatualizados;
iv. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
v. Portabilidade dos seus dados, mediante requisição expressa;
vi. Eliminação dos seus dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas na LGPD;
vii. Informação das entidades públicas e privadas com as quais a UFPR realizou uso compartilhado dos seus dados;
viii. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
ix. Revogação do consentimento, nos termos do art. 8º, § 5º, da LGPD.

2. Como você pode exercer seus direitos

Para o público interno, a confirmação de existência de maneira simplificada pode ser obtida através de opção específica em nossos sistemas internos.

Para público externo, ou para uma declaração completa e outras solicitações, elas poderão ser feitas através da plataforma FalaBR, criando uma solicitação para a UFPR com o assunto “Dados Pessoais – LGPD”, ou entrar diretamente em contato com o Serviço de Informação ao Cidadão – SIC:

Site: http://www.sic.ufpr.br/portal/
Endereço: Praça Santos Andrade, 50 - Prédio Histórico da UFPR – Térreo - CEP 80020-300 | Centro | Curitiba | PR | Brasil.
Fones: (41) 3310-2610/3310-2611.

O prazo de atendimento é de até 15 dias após o recebimento do pedido.

6. Da Segurança e da Proteção de seus Dados

A segurança de suas informações pessoais é importante para a UFPR. A UFPR adota os padrões de boas práticas para a proteção dos dados pessoais descritos em nossa Política de Segurança de Informação (PSI), em todo o ciclo de tratamento desses dados.

i. A UFPR não irá comercializar, alugar, ceder, ou emprestar os dados pessoais dos Titulares.
ii. A UFPR emprega as medidas apropriadas para proteger os dados pessoais contra riscos e ameaças à segurança da informação, como perda, uso indevido e acesso não autorizado, divulgação, alteração e destruição, levando em consideração os riscos envolvidos no processamento e a natureza dos dados pessoais;
iii. O Titular também é responsável pela proteção de seus dados, ficando atento a golpes, não compartilhando senhas pessoais, e tomando os devidos cuidados para manter seu computador pessoal e contas digitais seguros.

7. Da atuação perante a ANPD

i. A UFPR atuará sob as diretrizes com a Autoridade Nacional de Proteção de Dados para promover a proteção de dados pessoais nos limites da legislação vigente.
ii. A UFPR revisará suas diretrizes e procedimentos sempre que a ANPD exigir.
iii. Todas as solicitações e/ou questionamentos da ANPD serão prontamente respondidas pelo Encarregado de dados.

iv. Sempre que a ANPD solicitar a instauração de procedimento para averiguar qualquer situação envolvendo dados pessoais, como, mas não se limitando, ao descumprimento da LGPD, o Encarregado contará com o suporte do Comitê de Segurança da Informação.
v. Caberá somente ao Encarregado manter contato com a ANPD.

8. Disposições Gerais

i. A UFPR não utiliza qualquer tecnologia que infrinja qualquer legislação vigente ou esta Política, além de ter o objetivo de proteger os dados pessoais e garantir a privacidade dos Titulares.
ii. O Titular declara estar ciente de que a UFPR possui o direito de alterar o teor desta Política a qualquer momento, conforme a finalidade ou necessidade, como a adequação e a contínua conformidade à disposição de lei ou norma que tenha força jurídica equivalente. Cabe ao Titular verificar o conteúdo desta Política sempre que acessar o *website* da UFPR.
iii. Caso a Autoridade Nacional de Proteção de Dados ou uma decisão judicial repute que qualquer uma das disposições desta Política seja inadequada, inapropriada ou contrária a legislação vigente, as demais condições manterão vigência e pleno efeito.

9. Da Lei aplicável e foro

A presente Política de Privacidade será regida e interpretada segundo a legislação brasileira, no idioma português, sendo eleito o Foro da Comarca de domicílio do Titular para dirimir qualquer litígio ou controvérsia envolvendo o presente documento, salvo ressalva específica de competência pessoal, territorial ou funcional pela legislação aplicável.
Caso o Titular não possua domicílio no Brasil, será submetido à legislação brasileira, concordando, portanto, que em havendo litígio a ser solucionado, a ação deverá ser proposta no Foro da Cidade de Curitiba, estado do Paraná.

ANEXO II
POLÍTICA DE CONTROLE DE ACESSO

OBJETIVO

A presente política tem por objetivo estabelecer diretrizes para implementação de controles de acessos físicos e lógicos aos recursos de TIC (Tecnologia da Informação e Comunicação), relativos à Segurança da Informação, na Universidade Federal do Paraná, em conformidade com as necessidades institucionais e legais.

ABRANGÊNCIA

Esta política abrange os ativos de informação ofertados pela UFPR e deverá ser observada por todos os usuários desses ativos no âmbito da UFPR, sendo eles: Servidores Técnico-Administrativos ativos ou aposentados, Docentes ativos, aposentados ou substitutos em exercício, discentes ativos, Estagiários, Funcionários de empresas terceirizadas e/ou Prestadores de Serviços com contrato vigente e outros convidados externos atuando em atividades e projetos específicos de interesse da UFPR. Outros atores que necessitem de acesso a ativos de informações devem apresentar pedido fundamentado ao Gestor do Ativo de Informação, que decidirá pela aceitação ou negação do pedido.

TERMOS, CONCEITOS E DEFINIÇÕES

UFPR: Universidade Federal do Paraná.

TIC: Tecnologia da Informação e Comunicação.

AGTIC: Agência de Tecnologia da Informação e Comunicação. Órgão suplementar da UFPR, com a responsabilidade de direção, planejamento, desenvolvimento, execução, suporte e monitoramento das atividades relacionadas à TIC.

TIC descentralizada: unidade ou profissional de TIC de Setores Acadêmicos ou vinculadas/os à Reitoria, às Pró-Reitorias, às Superintendências ou a Agências da UFPR, exercendo atividades de Tecnologia da Informação e Comunicação externamente à AGTIC. As fundações de apoio, quando detentoras de ativos de informação da UFPR, também serão consideradas TIC descentralizadas para efeitos dessa Política;

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação da UFPR, observada eventual restrição que se aplique;

Ativos de Informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso. São exemplos de Ativos de Informação: computadores, impressoras, dispositivos de rede de dados (switches), servidores de arquivos, sistemas, aplicativos, bancos de dados, e-mail, intranet e internet, datacenter, racks e gabinetes de equipamentos, entre outros;

Controles de Acesso Físico: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, bloquear ou cancelar o acesso a ambientes, instalações e equipamentos de TIC. São exemplos de controles de acesso físico: controles de acesso a Datacenters através de biometria, controles de acesso aos racks, gabinetes e outros dispositivos de rede através de fechaduras.

Controles de Acesso Lógico: conjunto de procedimentos, recursos e meios com a finalidade de conceder, bloquear ou cancelar o acesso a dados, informações, banco de dados e sistemas. São exemplos de controle de acesso lógico: Controles de acesso à rede sem fio, controles de acesso a servidores de arquivos e sistemas acadêmicos e administrativos através de uma identificação de usuário protegida por senha.

Usuários: são as pessoas que possuem um vínculo ativo com a universidade e que fazem uso dos recursos de TIC para a execução de suas atividades.

Vínculo Ativo: relação formal e legítima de uma pessoa física ou jurídica com a UFPR, comprovada através de documentos válidos e atualizados que relacionem e justifiquem sua atividade com a UFPR, sejam elas de forma contratual, acadêmica ou funcional. Para fins desta política, os servidores aposentados do Regime Jurídico Único mantêm seu vínculo ativo com a UFPR.

Identificação do Usuário: é a provisão de uma identidade atribuída a um usuário que permite identificá-lo ao acessar um ativo de informação. Também denominada de login ou ID.

Autenticação: processo que busca verificar a identidade digital de um usuário de um sistema no momento em que ele requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pelo usuário com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo. Pode ser realizada através de recursos físicos ou lógicos como: senhas, tokens, biometria, entre outros, que sejam de conhecimento, posse ou características físicas exclusivas do

usuário.

Autorização: processo que ocorre após a autenticação e tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence. Portanto, autorização é o direito ou permissão de acesso a um recurso de um sistema;

Autoridade Responsável pelo Usuário: pessoa ou unidade ao qual o usuário está subordinado ou que mantém o vínculo ativo do usuário com a UFPR.

Gestores de Ativos de Informação: Responsáveis diretos por gerenciar um determinado ativo de informação, quer ele esteja custodiado pela AGTIC ou fora dela quando o gerenciamento do ativo ocorrer de forma descentralizada.

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

Tratamento (de dados pessoais): toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

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.

DIRETRIZES GERAIS

A Política de Controle de Acesso é componente fundamental para as demais normas relacionadas à Segurança da Informação e Comunicação e visa a estabelecer processos de concessões, alterações, bloqueios, cancelamentos e controles de modo a garantir que os usuários sejam adequadamente identificados, autenticados e com acessos autorizados somente ao necessário e suficiente para a execução de suas atividades.

Os acessos aos ativos de informação devem ser realizados de forma segura e responsável, devendo ser monitorados, rastreados e auditados, de forma a proteger os dados pessoais e institucionais e os ambientes físicos contra acessos e usos indevidos por pessoas não autorizadas, garantindo a confidencialidade, a integridade, a disponibilidade das informações e a conformidade com as normas vigentes.

Os controles de acessos devem ser robustos, empregando os conceitos de identificação do usuário, autenticação e autorização, primando pelo emprego de métodos e procedimentos modernos e seguros.

A presente norma deverá observar as boas práticas e referências amplamente aceitas para a área de Segurança da Informação, com ênfase para as orientações do Governo Federal, para a ISO 27001 e para a ISO 27002.

Quando os ativos de informação forem sistemas de informação (ou outras aplicações relevantes para o seu funcionamento - como bancos de dados, datacenters e equipamentos servidores) devem ser nominados e relacionados a Gestores.

O detalhamento dos recursos disponíveis bem como das orientações de acesso e uso são estabelecidos em políticas e procedimentos específicos elaborados e comunicados pelos Gestores de Ativos de Informação ou pela AGTIC.

GESTÃO DE ACESSO

Do Direito de Acesso

O Gestor de Ativo de Informação autorizará acesso aos ativos de informação de acordo com função, atribuição, responsabilidades e demais necessidades legítimas que justifiquem o acesso e pelo período em que o usuário possuir vínculo ativo com a UFPR.

Podem solicitar acesso os usuários que possuírem os seguintes Tipos de Vínculo com a UFPR, conforme abaixo:

1. Servidores técnico-administrativos ativos e aposentados.
2. Docentes ativos, aposentados e substitutos em exercício.
3. Discentes ativos.
4. Bolsistas.
5. Estagiários.
6. Funcionários de empresas terceirizadas ou prestadores de serviços com contrato em vigência.
7. Professores e pesquisadores visitantes.
8. Representantes da comunidade nos Conselhos Superiores.
9. Pesquisadores, prestadores de serviços ou participantes de eventos na UFPR.

Outros tipos de vínculos que venham a surgir e que sejam diferentes dos citados acima deverão ser tratados diretamente o Gestor de Ativo de Informação envolvido. Cabe ao referido Gestor informar a demanda à Direção da AGTIC para atualização da presente Política de Acesso junto ao Comitê competente.

Da Identificação de Acesso

A identificação do usuário deverá ser proporcionada por soluções que possibilitem uma gestão única de identidade, visando melhores controles de acesso, segurança e integração entre os recursos.

Da Concessão de Acesso

Cada Gestor de Ativo de Informação definirá os critérios de concessão de acesso a cada ativo de informação sob sua responsabilidade, informando à unidade ou pessoa responsável por sua operacionalização.

As informações e procedimentos de solicitação deverão estar disponíveis em locais de fácil acesso e de constante divulgação.

O acesso a um ativo de TIC somente será concedido ao usuário que possuir vínculo ativo com a UFPR conforme itens 1 a 8 acima e estará condicionada à aceitação de Termo de Responsabilidade, elaborado preferencialmente por meios digitais, no qual o usuário declarará estar ciente de suas responsabilidades e das normas vigentes referentes a Segurança da Informação e Comunicação, privacidade e de uso de ativos de informação.

A identificação e autenticação são etapas da gestão de acesso que já autorizam o uso das funcionalidades básicas definidas para o ativo de TIC disponibilizado. Conforme especificidade de cada ativo de TIC, procedimentos adicionais de autorização poderão ser necessários para que outras funcionalidades sejam liberadas ao usuário.

Dos Bloqueios, Cancelamentos ou Alterações de Acesso

Os acessos aos recursos de TIC poderão ser alterados, bloqueados temporariamente ou mesmo cancelados nas seguintes situações:

1. Por solicitação do próprio usuário detentor do acesso.
2. Por solicitação da autoridade responsável pelo usuário.
3. Por solicitação do próprio Gestor do Ativo de Informação em relação ao ativo sob sua responsabilidade.
4. Quando forem detectadas tentativas seguidas de acesso sem sucesso ou qualquer outra forma que caracterize suspeita de violação.
5. Quando for constatado o mau uso ou uso indevido do ativo.
6. Quando for alterado o tipo de vínculo que o usuário tiver com a UFPR, seu cargo ou função, ou mesmo as suas atribuições e responsabilidades.
7. Quando o usuário detentor do acesso deixar de possuir vínculo ativo com a UFPR.

Para possibilitar tratativas de interesse mútuo, um prazo adicional de 60 (sessenta) dias será atribuído após a data de encerramento dos vínculos mencionados nos itens 1 a 8, não caracterizando prorrogação de vínculo.

FORMAS DE AUTENTICAÇÃO DO USUÁRIO

A autenticação de usuários deve ser feita minimamente pela utilização do conjunto “usuário + senha” ou pela combinação de dois ou mais métodos (autenticação multifator), sendo esta última uma medida de segurança que deve ser buscada pela Universidade, a fim de aumentar a segurança dos acessos.

A senha é a forma mais comum de autenticação do usuário. Ela é pessoal, sigilosa, intransferível e de total responsabilidade do usuário que a criou, sendo proibido o seu compartilhamento com outros usuários, podendo este fato, caso ocorra, ser caracterizado como ilícito previsto na legislação vigente e passível de penalidades.

O uso de senhas contribui para a proteção dos dados do usuário e para a redução dos riscos de acessos indevidos e/ou não autorizados aos ativos de informação.

Devido à importância deste atributo, faz-se necessária a existência de procedimentos mínimos e padronizados para a criação de senhas de acesso aos ativos de informação.

A criação de senhas deverá atender **no mínimo** os seguintes requisitos:

1. Somente será permitida a criação de senhas fortes, devendo estas conter, no mínimo, 8 (oito) caracteres, utilizando no mínimo 3 (três) das seguintes combinações: letras maiúsculas, letras minúsculas, números e caracteres especiais.
2. Quando necessária a criação de senhas temporárias de acesso, estas também deverão ser senhas fortes com obrigatoriedade de alteração no primeiro acesso.
3. As senhas deverão ser trafegadas e armazenadas de forma criptografada.
4. O próprio usuário deverá poder alterar a sua senha de acesso a qualquer momento.
5. Não permitir repetição de senhas.

RESPONSABILIDADES

Dos Usuários

1. Manter-se informado sobre as normas vigentes relacionadas a esta Política, assim como de suas atualizações.
2. Zelar pelo bom uso dos ativos de informação e em conformidade com suas atividades, com os interesses institucionais e com as normas vigentes.
3. Não compartilhar suas credenciais de acesso com terceiros.
4. Utilizar senhas fortes, seguras e protegê-las de forma apropriada.
5. Utilizar recursos/ferramentas institucionais para salvar, compartilhar e transferir arquivos e e-mails.
6. Utilizar preferencialmente os recursos institucionais para troca de mensagens relacionadas ao trabalho.
7. Comunicar formalmente sua Chefia Imediata, Gestores do Ativo de Informação e a AGTIC sobre qualquer irregularidade que houver percebido no uso do ativo.
8. Comunicar formalmente sobre eventuais fragilidades de segurança detectadas ou que tenha tido ciência e não as explorar.
9. Não repassar informações às quais tenha acesso para pessoas não autorizadas.
10. Não violar as regras de controle estabelecidas para o uso do ativo de informação.
11. Classificar as informações conforme sua sensibilidade e mantê-las protegidas de acordo com o nível de segurança exigido por elas.
12. Efetuar o bloqueio de acesso aos equipamentos quando não estiverem em uso, evitando acessos não autorizados.
13. Manter documentos e outras informações sigilosas protegidas em seu local de trabalho evitando deixá-los em local visível de fácil acesso.
14. Não gravar dados e/ou informações sensíveis em dispositivos que não possuam segurança apropriada, como por exemplo mídias removíveis, como pendrives, HDs externos ou outros.
15. Manter seus dados cadastrais atualizados na unidade responsável.

Das Autoridades Responsáveis

1. Assegurar que os colaboradores sob sua responsabilidade tenham conhecimento desta política e das demais relacionadas à Segurança da Informação e Comunicação.
2. Assegurar a concessão e a restrição dos acessos aos colaboradores sob sua responsabilidade de acordo com as especificidades da atividade desempenhada.
3. Comunicar aos Gestores de Ativos de Informação sobre quaisquer irregularidades no uso dos ativos de informação e tomar as providências disciplinares previstas.
4. Fornecer as documentações que comprovem o vínculo ativo de um usuário sob sua responsabilidade, quando solicitadas.
5. Comunicar formalmente sobre eventuais fragilidades de segurança detectadas ou que tenha tido ciência e não as explorar.
6. Promover a cultura da segurança da informação e comunicação nas suas unidades e garantir a implementação das políticas e leis a ela relacionadas.

Dos Gestores de Ativos de Informação

1. Prover o controle de acesso aos ativos de informação sob sua responsabilidade de forma a garantir o uso adequado e seguro do ativo através de mapeamentos e análises de risco compatíveis com sua criticidade e exigências de Segurança da Informação.
2. Definir procedimentos e requisitos de acesso e de revogação de acessos aos ativos de informação sob sua responsabilidade, observando os

dispositivos legais e regimentais relativos à confidencialidade, integridade e disponibilidade das informações.
3. Estabelecer mecanismos de coleta da ciência dos usuários, preferencialmente por meios digitais, quanto aos procedimentos e requisitos de acesso aos ativos de informação sob sua responsabilidade.
4. Conceder o acesso solicitado após cientificação dos usuários.
5. Bloquear ou cancelar o acesso aos ativos de informação quando solicitado pelo próprio usuário, pela autoridade responsável pelo usuário ou de forma autônoma e de caráter preventivo, quando for detectado o mau uso do ativo, devendo nesse caso, informar imediatamente a autoridade responsável pelo usuário.
6. Tomar as providências necessárias para que sejam mantidas a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações disponibilizadas pelo ativo de informação, de acordo com as normas vigentes.
7. Prover controles que permitam o registro, monitoramento, rastreabilidade, prevenção e auditoria dos acessos aos ativos de informação, principalmente os críticos, zelando pelos prazos legais de manutenção dessas informações.
8. Fornecer os registros de acesso e uso, quando solicitados por autoridade competente e nas formas legais.
9. Aplicar medidas preventivas e/ou corretivas que eliminem ou reduzam os riscos de acessos indevidos.

Dos Gestores de Contratos de Serviços de TIC com Terceiros

1. Fazer com que esta política e as demais normas de TIC sejam de conhecimento das empresas e de prestadores de serviços, devidamente registrado em contrato, caso seja prevista a necessidade de acesso aos ativos de informação da UFPR para a execução dos serviços contratados.
2. Providenciar o acesso e restrição de prestadores de serviço aos ativos de informação da UFPR necessários à execução do serviço terceirizado.
3. Tomar providências cabíveis junto à contratada quando for observado o mau uso de ativo de informação da UFPR.
4. Solicitar o cancelamento dos acessos ao término do contrato de serviço.

Das Unidades de TIC Descentralizadas

1. Garantir que as ações das suas unidades de TI descentralizadas estejam alinhadas com esta política e com as demais normativas relativas à Segurança da Informação e Comunicação da UFPR.

Da Direção da AGTIC

1. Manter esta política atualizada e alinhada com as necessidades institucionais e legais.
2. Divulgar periodicamente esta política através dos canais oficiais da UFPR.
3. Fomentar o desenvolvimento de projetos que promovam a melhoria contínua nos controles de acesso.

Da Equipe de Tratamento de Incidentes de Segurança da Informação

1. Receber as comunicações de incidentes oriundas de irregularidades de acesso e tomar as medidas cabíveis, em consonância com o Plano de Resposta de Incidentes.

Do Subcomitê de Segurança da Informação e Privacidade

1. Aprovar, promover e acompanhar a aplicação da presente Política no âmbito da UFPR.
2. Apreciar e aprovar alterações da Política.
3. Propor melhorias, alterações e adequações nesta Política.

SANÇÕES DISCIPLINARES

Em casos comprovados de mau uso dos ativos de informação, o acesso poderá ser bloqueado ou cancelado e as informações sobre a infração serão fornecidas pelo Gestor do Ativo de Informação às autoridades responsáveis para que sejam tomadas as providências disciplinares previstas.

ANEXO III
POLÍTICA DE USO DE RECURSOS DE TIC

OBJETIVO

Esta política tem por objetivo estabelecer diretrizes referentes à utilização dos ativos de informação relacionados à TIC, físicos e lógicos, no âmbito da Universidade Federal do Paraná, a fim de proporcionar a redução de riscos por uso indevido, bem como a redução de ocorrência de incidentes e ameaças, internas ou externas, provocadas ou acidentais, que possam causar danos à Segurança da Informação e Comunicação e ao patrimônio da instituição, em conformidade com as necessidades institucionais e legais.

ABRANGÊNCIA

Esta política abrange os ativos de informação ofertados pela UFPR e deverá ser observada por todos os usuários desses ativos no âmbito da UFPR, sendo eles: Servidores Técnico-Administrativos ativos ou aposentados, Docentes ativos, aposentados ou substitutos em exercício, discentes ativos, estagiários, funcionários de empresas terceirizadas e/ou prestadores de serviços com contrato vigente e outros convidados externos atuando em atividades e projetos específicos de interesse da UFPR.

TERMOS, CONCEITOS E DEFINIÇÕES

AGTIC: Agência de Tecnologia da Informação e Comunicação. Órgão suplementar da UFPR, com a responsabilidade de direção, planejamento, desenvolvimento, execução, suporte e monitoramento das atividades relacionadas à TIC.

Áreas Desprotegidas: Para fins desta política, são consideradas áreas desprotegidas aquelas cujos processos de segurança da informação possuem vulnerabilidades (falhas ou fraquezas) que podem ser exploradas por ameaças internas ou externas, como invasões por programas mal-intencionados, falhas ou ausências de cópias de segurança, defeitos diversos no hardware do equipamento (queima de placas, discos ou pen drives) que resultem danos indesejados e/ou irreparáveis.

Autoridade Responsável pelo Usuário: Pessoa ou unidade ao qual o usuário está subordinado ou que mantém seu vínculo ativo com a UFPR.

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

Base de Dados: Conjunto de dados inter-relacionados, organizados de maneira a permitir a recuperação da informação e armazenados por meios ópticos, magnéticos ou eletrônicos, sendo acessados de forma local ou remota.

Código-Fonte: É um conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções de maneira lógica, em uma das linguagens de programação existentes.

Conexão P2P: Forma de conexão de rede ponto a ponto que conecta quaisquer computadores de forma descentralizada com o objetivo de realizar downloads de arquivos.

CSA: Seção de Central de Serviços e Atendimento em TIC. Unidade da AGTIC responsável por prestar atendimento e suporte técnicos aos usuários de recursos de TIC gerenciados pela AGTIC.

Dados: São partes isoladas e brutas de informação não tratada e armazenadas que por si só não possuem um significado ou um contexto que permita sua compreensão.

Datacenter: Trata-se de ambiente físico projetado para abrigar e concentrar, de forma adequada e segura, equipamentos necessários para o armazenamento de dados e sistemas, gerenciamento de servidores, rede e telecomunicações, além de realizar o processamento de informações.

Demais Colaboradores: para efeitos dessa política, um conjunto de pessoas que trabalha em determinada organização pública, exercendo atividades cujos vínculos podem ser classificados como funcionários, empregados, prestadores de serviços terceirizados, estagiários, entre outros, exceto o vínculo de Servidor Público.

Dispositivos de Rede: São os equipamentos que facilitam e dão suporte ao uso de uma rede de computadores, interconectando os dispositivos.

Dispositivos sem fio: São equipamentos que possuem a capacidade de se comunicar com uma rede, transferindo dados ou informações, sem a necessidade de cabos conectados fisicamente.

Gestores de Recurso: Responsáveis diretos por gerenciar um determinado recurso de TIC. Em sua maioria pertencem à estrutura funcional da AGTIC, porém, podem também pertencer a outra unidade da UFPR, quando o gerenciamento do recurso ocorrer de forma descentralizada.

Hardware: Conjunto de componentes que compõem a parte física de computadores ou equipamentos de tecnologia, como placas, impressoras, processadores, monitores, entre outros.

Informação Confidencial: Trata-se da informação cujo conhecimento não esteja disponível ou não seja revelado a pessoa, a sistema, a órgão ou entidade não autorizados nem credenciados.
Informação: São dados processados e tratados de forma a terem um significado que permitam sua compreensão.

Monitoramento do Parque Computacional: Para fins desta política, trata-se de monitoramento realizado de forma informatizada e em tempo real, em todo o conjunto de equipamentos e softwares utilizados em tecnologia da informação e comunicação e interconectados na rede de dados institucional, com o objetivo de montar um inventário de TIC por meio da obtenção de uma lista detalhada dos recursos de tecnologia tais como, computadores, notebooks, impressoras, câmeras, roteadores, switches, modens, antenas, servidores, racks, programas, licenças de uso, serviços em nuvem, entre outros. O inventário de TIC possui a finalidade de auxiliar a gestão de TIC na tomada de decisões estratégicas, facilitar o gerenciamento de prazos e garantias e a detecção de problemas e não se confunde com inventário patrimonial, cujos objetivos são fiscais e contábeis.

Proxies: Proxy é um serviço que age como intermediário entre o usuário e a internet, recebendo e repassando as requisições ao site de internet que está sendo acessado.

Recursos de TIC: Conjunto de equipamentos e soluções que proporcionam a produção, o armazenamento, a transferência, o acesso, a segurança e o uso de dados e informações. Apresentam-se subdivididos nas formas física, como computadores, impressoras, dispositivos de rede de dados, servidores de arquivos, datacenters, racks e gabinetes de equipamentos, entre outros e lógica, como sistemas, aplicativos, bancos de dados, e-mail, acesso à intranet e internet, entre outros.

RNP: Rede Nacional de Ensino e Pesquisa.

RJU: Regime Jurídico Único. É o regime jurídico dos servidores públicos civis da administração direta, das autarquias e das fundações, instituído pela Lei n.º 8.112/90. O RJU regula a relação entre os servidores públicos e a administração.

Servidor Público: Pessoas físicas ocupantes de cargos públicos providos por concurso público conforme Art. 37, Inciso II da Constituição Federal de 1988, regidos por um estatuto que define direitos e obrigações.

Sites: São endereços eletrônicos ou um conjunto de páginas web disponíveis na rede mundial de computadores (internet) ou em redes privadas (intranet).

Software: Conjunto de instruções executadas por um dispositivo com capacidade de interpretá-las e processá-las, como computadores ou smartphones, com o objetivo de produzir comportamentos e resultados específicos. Abrange os sistemas operacionais, aplicativos para computadores e celulares, sistemas administrativos, sistemas acadêmicos, entre outros.

TIC: Tecnologia da Informação e Comunicação.

TIC descentralizada: unidade ou profissional de TIC de Setores Acadêmicos ou vinculados à Reitoria, às Pró-Reitorias, às Superintendências ou a Agências da UFPR, exercendo atividades de Tecnologia da Informação e Comunicação externamente à AGTIC. As fundações de apoio, quando detentoras de ativos de informação da UFPR, também serão consideradas TIC descentralizadas para efeitos dessa Política;

Tratamento de dados pessoais : Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Usuários: São as pessoas que possuem um vínculo ativo com a universidade e que fazem uso dos recursos de TIC para a execução de suas atividades.

Vínculo Ativo: Relação formal e legítima de uma pessoa física ou jurídica com a UFPR, comprovada através de documentos válidos e atualizados que relacionem e justifiquem sua atividade com a universidade, seja ela de forma contratual, acadêmica ou funcional. Para fins desta política, preservadas as exceções expressas, os servidores aposentados do Regime Jurídico Único (RJU) mantêm seu vínculo ativo com a UFPR.

DIRETRIZES GERAIS

Os recursos de TIC fornecidos pela UFPR, tanto os físicos como os lógicos, são de uso exclusivo para o desenvolvimento de atividades essenciais e vinculadas aos interesses institucionais, sendo essas atividades relacionadas ao ensino, pesquisa, extensão, inovação e às atividades administrativas.

Os recursos de TIC são disponibilizados pela AGTIC ou pelas Unidades de TIC Descentralizadas, que são responsáveis por administrá-los, monitorá-los, garantir sua integridade, disponibilidade e segurança, bem como prestar o suporte aos seus usuários.

Formas de solicitações, concessões, alterações, bloqueios e cancelamentos dos acessos aos recursos de TIC, bem como informações relacionadas a grupos, perfis e permissões, são estabelecidas em políticas e procedimentos específicos, em conformidade com esta e demais normas vigentes da UFPR.

Manuais de usuário com informações sobre o uso do recurso deverão ser elaborados, divulgados e disponibilizados pelos gestores do recurso em locais de fácil acesso e mantidos constantemente atualizados em conformidade com esta política e demais vigentes.

O uso de qualquer recurso de TIC poderá ser monitorado e auditado com as finalidades de garantir seu uso adequado, evitar danos financeiros, operacionais ou outros que causem impactos negativos à imagem da UFPR, em conformidade com as normas vigentes.

A AGTIC, em conformidade com as boas práticas de TIC, com as recomendações dos órgãos de controle e com as políticas de TIC do Governo Federal, manterá o monitoramento do parque computacional, conforme glossário, de forma automatizada e centralizada.

É vedado o uso de qualquer mecanismo que vise burlar credenciais de acesso, capturar dados não autorizados, causar danos físicos, gerar sobrecarga de uso ou qualquer outro que caracterize fraude, sabotagem ou riscos à segurança da informação e comunicação.

Caso seja evidenciado o uso inadequado do recurso de TIC por um determinado usuário, o gestor do recurso poderá bloquear temporariamente o uso desse recurso, comunicando o fato às autoridades responsáveis por este usuário, para que sejam tomadas as providências disciplinares previstas.

O uso de qualquer recurso de TIC fornecido pela UFPR, explicitamente citado ou não nesta política, está sujeito aos ditames da legislação pertinente, da proteção de direitos autorais, de imagem, da proteção e tratamento de dados pessoais, da privacidade e da segurança da informação e comunicação.

É vedado o uso de qualquer recurso, mecanismo ou ferramenta que permita divulgação e/ou compartilhamento de dados, arquivos ou informações classificadas ou entendidas como confidenciais, para outrem não expressamente autorizados a conhecê-las.

Dados e informações digitais armazenados nos ativos disponibilizados pela UFPR que sejam essenciais para continuidade das atividades da UFPR são considerados como pertencentes à administração pública, sendo vedada a restrição de acesso aos mesmos pelos seus detentores, salvo para cumprimento de obrigação legal ou regulatória.

DO USO DE DISPOSITIVOS DE USUÁRIO FINAL

São considerados dispositivos de usuário final os computadores de mesa, computadores portáteis, *tablets*, *smartphones* e outros caracterizados como de uso individual, de propriedade da UFPR ou de propriedade do próprio usuário no ambiente de rede da UFPR.

Os dispositivos de usuário final de propriedade da UFPR são preparados de forma padronizada com configurações de hardware, sistema operacional e programas instalados pré-definidos pela unidade de TIC responsável. O acesso a esses dispositivos deverá ser efetuado de forma segura, através de credenciais de acesso individuais e em conformidade com as políticas de segurança e de acesso vigentes.

É vedado ao usuário o privilégio de administração e o acesso à senha do administrador local do dispositivo de usuário final de propriedade da UFPR, exceto nos casos autorizados pela AGTIC ou pelo responsável pela unidade de TIC local.

É permitido o uso de dispositivos de usuário final de propriedade do próprio usuário no ambiente de rede da UFPR. Nesse caso, os serviços de suporte da AGTIC e das unidades de TIC descentralizadas estarão limitados apenas ao fornecimento de orientações sobre as configurações necessárias para conexão à rede de dados institucional e aos sistemas institucionais. Uma vez conectado à rede privada da UFPR, seu uso deve ser limitado aos interesses institucionais e regido conforme normas internas vigentes.

A AGTIC ou as unidades de TIC descentralizadas poderão bloquear o acesso à rede e aos sistemas de um dispositivo de usuário final quando forem detectadas irregularidades, tais como: não atender aos requisitos mínimos de configuração, falta de atualização do sistema operacional, ausência de softwares antivírus, geração suspeita de tráfego de dados, cópias, armazenamento e transferência de dados institucionais sensíveis e/ou pessoais sem autorização ou outras irregularidades que coloquem em risco a segurança da informação e comunicação.

A AGTIC ou a unidade de TIC responsável deverá definir e executar os procedimentos necessários e seguros para descartar as informações contidas em um dispositivo de usuário final de propriedade da UFPR antes de efetuar a sua realocação, envio para assistências técnicas ou descarte definitivo por danos ou obsolescências.

DOS RECURSOS DE ARMAZENAMENTO E COMPARTILHAMENTO DE DADOS

Todas as informações institucionais digitais ou digitalizadas devem ser armazenadas e/ou compartilhadas valendo-se de recursos e ferramentas homologados e disponibilizados pela AGTIC ou pela unidade de TIC Descentralizada, recursos esses de propriedade ou sob gestão da UFPR que deverão prover os mecanismos necessários para a salvaguarda e compartilhamento das informações.

A AGTIC não se responsabilizará por informações armazenadas em ferramentas não disponibilizadas pela mesma.

É vedado o compartilhamento de dados e/ou arquivos produzidos ou gerados em decorrência das atividades institucionais como documentos, atas, memória de reuniões, planilhas, apresentações, fotos, áudios, vídeos, entre outros, ou ainda protegidos, sem a expressa autorização de seus autores ou em desacordo com a Lei de Acesso a Informação e Lei Geral de Proteção de Dados Pessoais, respeitado o princípio da transparência no que couber.

Não é recomendado o armazenamento e/ou compartilhamento de dados institucionais em áreas desprotegidas, tais como unidades internas de computadores, dispositivos externos portáteis ou dispositivos de propriedade do próprio usuário.

DA UTILIZAÇÃO DA REDE DE DADOS INSTITUCIONAL

A Rede de Dados Institucional é uma rede privada e administrada de forma centralizada pela AGTIC, com o objetivo de permitir o tráfego de dados e o acesso à internet, intranet, sistemas, aplicativos e demais recursos disponibilizados para uso em rede.

A conexão de dispositivos de usuário final, na Rede de Dados Institucional, é possibilitada de forma cabeada ou por intermédio de dispositivos sem fio.

A cada ponto de acesso físico da rede de dados da UFPR poderá ser conectado apenas um dispositivo de usuário final, sendo proibida a conexão de quaisquer outros tipos de dispositivo de rede, como *hubs*, *switches*, *access points*, roteadores, entre outros, salvo mediante expressa autorização da AGTIC. Uma vez autorizados, esses dispositivos passam a ser regidos por esta política e demais regulamentações internas.

O monitoramento da Rede de Dados Institucional é de responsabilidade da AGTIC, que poderá, sempre que se fizer necessário, adotar medidas tais como: bloqueios totais ou parciais de acesso à rede, priorizar o tráfego de aplicações críticas, limitar a largura da banda da rede, entre outros, a fim de garantir o atendimento às necessidades institucionais.

É terminantemente vedado o uso de recursos de tecnologia não autorizados formalmente pela AGTIC com o objetivo de analisar e monitorar o tráfego da Rede de Dados Institucional.

Qualquer necessidade de contratação de provedores de acesso à internet deve ser previamente autorizada pela AGTIC.

DO USO DA INTERNET

O acesso à internet é fornecido exclusivamente pelos meios autorizados e configurados pela AGTIC, sendo expressamente vedado o uso de soluções de burla, como *proxies* externos ou similares.
É proibido o acesso a sites cujo conteúdo for considerado incompatível com as atividades institucionais da UFPR ou em desacordo com as normas e leis vigentes ou que representem ameaça à segurança da informação e comunicação.

A AGTIC, sempre que necessário e dentro dos interesses institucionais, poderá bloquear acessos a serviços e páginas da internet que estiverem em desacordo com as normas vigentes ou que onerem o tráfego de rede de forma a prejudicar o bom andamento das atividades da UFPR ~~a exemplo de fluxo de áudio e vídeo em tempo real.~~

Casos omissos, ou que demandem acesso a conteúdos que por ventura sejam proibidos ou restritos pelas regras institucionais aplicadas pela AGTIC, deverão ser encaminhadas à Direção Executiva da mesma, justificativas institucionais suficientes para liberação.

O acesso aos recursos de internet deverá estar em consonância com as normas da RNP.

DO USO DO CORREIO ELETRÔNICO

Todo o usuário, em conformidade com a Política de Acesso, terá um endereço de e-mail institucional com o domínio " **@ufpr.br**".

É **obrigatório o uso do e-mail institucional** para todas as comunicações oficiais internas ou externas, visando garantir a autenticidade, integridade, confiabilidade, segurança e o não repúdio das comunicações.

A AGTIC poderá definir quotas iniciais de utilização de e-mail com a finalidade de garantir a disponibilidade e qualidade do serviço de correio eletrônico. Alterações de quotas poderão ser solicitadas e estarão condicionadas à análise e viabilidade técnicas.

O acesso ao e-mail poderá ocorrer por meio de uma interface web ou por intermédio de aplicativos homologados valendo-se de qualquer dispositivo conectado à internet. Cabe ao usuário adotar todas as recomendações de segurança, principalmente quando se tratar de uma rede de dados e de dispositivos de uso público.

ENDEREÇO DE E-MAIL DEPARTAMENTAL

E-mails departamentais (unidade, equipe, comissão/comitê, projetos, entre outros) poderão ser criados mediante solicitação de servidores ativos pertencentes ao quadro RJU, que terão seu CPF (titularidade) vinculados ao e-mail solicitado durante a vigência de sua responsabilidade pelo mesmo.

Contas departamentais poderão ter sua titularidade transferida a outro servidor
nos casos de alteração de responsabilidade ou interesse institucional.

GRUPOS/LISTAS DE E-MAIL

A AGTIC criará e gerenciará listas de e-mail para comunicações oficiais da UFPR, no mínimo para as categorias de discentes, docentes e servidores técnico-administrativos.

DO USO DOS RECURSOS DE IMPRESSÃO E DIGITALIZAÇÃO

A utilização desses recursos deve ser pautada na sustentabilidade ambiental com foco no uso consciente, evitando impressões desnecessárias de documentos, reduzindo custos operacionais e financeiros.

Os recursos de impressão e digitalização devem ser utilizados única e exclusivamente para fins institucionais e por colaboradores com vínculo ativo. Seu uso é vedado por discentes, exceto quando estes estejam atuando como estagiários ou bolsistas com vínculos devidamente formalizados.

A AGTIC poderá disponibilizar, mediante solicitação e aprovação, equipamentos de impressão e digitalização, para uso em rede e de forma compartilhada, destinados a uma unidade ou a um grupo de trabalho, provendo mecanismos de segurança para o tratamento de documentos sigilosos ou sensíveis sempre que se fizer necessário.

É vedado o fornecimento de equipamentos única e exclusivamente para utilização individual ou que estes sejam instalados em locais restritos e de difícil acesso, impedindo dessa forma a sua utilização e compartilhamento adequados.

Sempre que possível, serão disponibilizados equipamentos que possuam controle de acesso e recursos de impressão frente e verso.

Quando disponível, a impressão em cores deve ser utilizada apenas nos casos de extrema necessidade e nas versões finais do documento.

O reabastecimento de papel é de responsabilidade do usuário devendo este sempre utilizar os tipos recomendados, evitando o uso daqueles que estejam fora das especificações da impressora e evitando também o uso de papéis amassados, sujos ou úmidos, que podem causar o atolamento e danos ao equipamento.

O monitoramento do uso dos equipamentos de impressão e digitalização é de responsabilidade da AGTIC, que disponibilizará relatórios periódicos de utilização, sempre que solicitado ou quando for observado o uso indevido ou inadequado do equipamento.

DO USO DE PRODUTOS DE SOFTWARE

A UFPR recomenda a utilização de softwares livres sempre que possível.

Todo produto de software a ser utilizado no ambiente da UFPR, seja ele comercial, livre ou desenvolvido internamente, terá seu uso permitido desde que possua relação direta com as atividades institucionais da UFPR e respeite todas as cláusulas referentes à propriedade, ao licenciamento, à cópia, reprodução e distribuição.

A UFPR não é responsável pelo licenciamento ou manutenção de produtos de software instalados nos dispositivos de propriedade do usuário.

Devido à necessidade legal de controle de ativos de TIC pelos órgãos da Administração Pública, licenciamentos de software providos pela UFPR não podem ser instalados em equipamentos de propriedade do usuário, exceto aqueles homologados que sejam de uso gratuito.

Não é permitida a instalação de produtos de software nos equipamentos de propriedade da instituição sem que possuam o devido licenciamento em nome da UFPR ou sem expressa autorização da AGTIC ou da unidade de TIC Descentralizada.

Ainda que o usuário seja autorizado a instalar produto de software adquirido, o licenciamento e manutenção do mesmo são de sua responsabilidade.

Não é permitida a instalação de produtos de software não homologados nos dispositivos da UFPR, sem a devida autorização da AGTIC ou da unidade de TIC Descentralizada responsável pelo equipamento, que deverão manter uma lista atualizada dos softwares homologados em local de fácil acesso para consulta.

A AGTIC ou a unidade de TIC responsável poderão bloquear ou desinstalar os softwares que estiverem em desacordo com esta política.

PRODUTOS DE SOFTWARE DESENVOLVIDOS INTERNAMENTE E SITES HOSPEDADOS

A hospedagem dos produtos de software e sites institucionais nos servidores de rede e bancos de dados será regida por normas específicas, a serem elaboradas pelo SETIC.

DOS DEMAIS RECURSOS DE TIC

Outros recursos de TIC, não explicitamente citados, são regidos pelas diretrizes gerais desta política.

São de responsabilidade da AGTIC ou das Unidades de TIC descentralizadas, elaborar, divulgar e manter uma relação atualizada dos recursos de TIC, os quais gerenciam, em local público e de fácil acesso.

DO SUPORTE AO USO DOS RECURSOS DE TIC

O suporte deverá ser viabilizado e prestado pela unidade gestora do recurso, que deverá estabelecer, manter, disponibilizar e divulgar os canais de suporte para atendimento aos seus usuários.

Os canais de suporte se destinarão somente ao atendimento aos usuários cujos recursos de TIC são comprovadamente de propriedade ou de responsabilidade da UFPR. Não será fornecido suporte a recursos de TIC de propriedade do próprio usuário.

É terminantemente vedado ao usuário abrir equipamentos, desconectar cabos de dados ou de energia, retirar peças/componentes, alterar suas configurações originais ou qualquer outro ato que vise reparar problemas ou falhas nos Recursos de TIC, sem que tenha sido previamente orientado pelo suporte técnico ou que tenha sido previamente autorizado e treinado. Em caso de dúvidas ou problemas, o usuário deve, primeiramente, acionar os canais de suporte disponíveis.

Nos casos em que o usuário utilize equipamento próprio para as necessidades institucionais, será prestado suporte apenas em relação a softwares e sistemas executando nesses equipamentos, sendo vedado à UFPR qualquer manutenção de hardware, sistema operacional ou outros softwares que não sejam de propriedade ou licenciados pela UFPR.

DAS PERDAS, DANOS, FURTOS OU ROUBOS

Nos casos de perdas, danos, furtos ou roubos, caberá ao usuário comunicar imediatamente a unidade gestora do recurso para que sejam executadas as medidas de prevenção cabíveis contra o uso indevido por terceiros, assim como comunicar os responsáveis pela segurança patrimonial para que tomem as medidas previstas.

A reposição do recurso dependerá de disponibilidade e da aprovação da sua unidade de TIC gestora para a substituição.

DAS RESPONSABILIDADES

Dos Usuários

1. Manter-se informado sobre as normas vigentes relacionadas a esta política, assim como de suas atualizações.
2. Zelar pelo bom uso do recurso de TIC, por sua integridade física e pela Segurança da Informação e Comunicação ao utilizá-lo.
3. Utilizar os recursos de TIC disponíveis sempre em conformidade com suas atribuições e no desempenho de suas atividades, com os interesses institucionais e com as normas vigentes.
4. Atender a legislação vigente, as normativas específicas da UFPR, bem como a quaisquer requisitos de Segurança da Informação e Comunicação definidos pelos Gestores dos Recursos de TIC de que fizerem uso.
5. Comunicar imediatamente à sua Chefia Imediata, aos Gestores do Recurso, à AGTIC ou à Unidade de TIC descentralizada, quaisquer irregularidades que houver percebido no uso do recurso de TIC.
6. Comunicar imediatamente à sua Chefia Imediata, aos Gestores do Recurso, ao suporte, à AGTIC ou à Unidade de TIC descentralizada,

eventuais fragilidades de Segurança da Informação e Comunicação, relacionadas ao recurso de TIC, que tenha identificado ou que tenha tido ciência e não as explorar.
7. Solicitar formalmente o suporte técnico da área responsável quando constatar ou tiver conhecimento de problemas, erros, falhas ou mesmo dúvidas relacionadas ao funcionamento dos recursos de TIC de que fizerem uso.
8. Não abrir equipamentos, desconectar cabos de dados ou de energia, retirar peças/componentes, alterar suas configurações originais ou qualquer outro ato que vise a reparar problemas ou falhas nos Recursos de TIC.
9. Não violar as regras de controle estabelecidas, bem como as características técnicas específicas e necessárias para o bom funcionamento de cada recurso de TIC.
10. Efetuar o bloqueio de acesso aos equipamentos quando não estiverem em uso, evitando acessos não autorizados.
11. Não gravar dados e/ou informações sensíveis em dispositivos que não possuam segurança apropriada, como dispositivos móveis de armazenamento do tipo Pendrives e HDs Externos.
12. Manter seus dados cadastrais atualizados na unidade responsável.
13. Garantir a proteção e o zelo dos dados ou informações das quais tenha conhecimento e/ou acesso.
14. Responder por situações em que for evidenciado dano em decorrência do descumprimento dos ditames dessa política e demais normas vigentes.

Das Chefias e demais Autoridades Responsáveis

1. Assegurar que os servidores e/ou colaboradores e/ou demais usuários sob sua responsabilidade tenham conhecimento desta política e das demais relacionadas à Segurança da Informação e Comunicação.
2. Assegurar que os servidores e/ou colaboradores e/ou demais usuários sob sua responsabilidade utilizem os recursos de TIC de forma adequada e segura.
3. Autorizar o acesso, alterar as permissões, bloquear ou cancelar credenciais de usuários para determinados recursos de TIC, quando solicitado pelos Gestores de Recursos de TIC.
4. Comunicar aos Gestores de Recursos de TIC sobre eventuais movimentações ocorridas na equipe que impliquem perda de acesso a recursos de TIC por desvinculação da unidade.
5. Comunicar aos Gestores de Recursos de TIC quaisquer irregularidades constatadas ou de que tiver ciência no uso de recursos e tomar as providências disciplinares previstas.
6. Fornecer as documentações que comprovem o vínculo ativo de um usuário sob sua responsabilidade, quando solicitado.
7. Comunicar formalmente à AGTIC, o Gestor do Recursos ou à Unidade de TIC Descentralizada sobre eventuais fragilidades de Segurança da Informação e Comunicação detectadas ou que tenha tido ciência e não as explorar.

Dos Gestores de Recursos

1. Prover o controle de acesso aos recursos de TIC de forma a garantir o uso adequado e seguro desses recursos por meio de mapeamentos e análises de riscos e infraestruturas física e lógica compatíveis com sua criticidade e exigências de Segurança da Informação e Comunicação.
2. Garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações disponibilizadas pelo recurso de TIC, de acordo com as normas vigentes.
3. Prover controles que permitam o registro, monitoramento, rastreabilidade, prevenção e auditoria dos dados referentes a utilização dos recursos de TIC, principalmente aqueles críticos, zelando pelos prazos legais de manutenção dessas informações.
4. Manter os registros de utilização dos recursos de TIC em locais seguros, respeitando os prazos legais.
5. Fornecer os registros de acesso e uso, sempre que solicitado por autoridade competente e nas formas legais.
6. Aplicar medidas preventivas e/ou corretivas que eliminem ou reduzam os riscos de acessos e utilização indevidos aos Recursos de TIC.
7. Acompanhar as auditorias internas e externas, fornecendo as informações solicitadas e em conformidade com as normas vigentes.
8. Elaborar, divulgar e disponibilizar manuais e orientações de utilização dos recursos de TIC, em locais de fácil acesso e mantê-los constantemente atualizados.
9. Garantir que os recursos de TIC estejam disponíveis, seguros, inclusive por meio de cópias de segurança, atualizados e íntegros, contribuindo assim para desenvolvimento e a continuidade das operações diárias da UFPR que utilizam tais recursos.
10. Manter as equipes de atendimento e suporte atualizadas acerca das alterações nos procedimentos de acesso e utilização dos Recursos de TIC.
11. Fornecer informações e aplicar medidas determinadas pela AGTIC que tenham como objetivo manter o monitoramento centralizado do parque computacional da UFPR.

Das Equipes de Atendimento e Suporte

1. Fornecer orientações e suporte aos usuários utilizadores dos recursos de TIC de propriedade ou responsabilidade da UFPR, quando formalmente solicitado por intermédio dos canais disponíveis.

Dos Gestores de Contratos de Serviços

1. Fazer com que esta política e as demais normas de TIC sejam de conhecimento das empresas e Prestadores de Serviços caso seja previsto a necessidade de acesso aos recursos de TIC para a execução dos serviços contratados.
2. Autorizar o acesso de funcionários e Prestadores de Serviço.
3. Solicitar alteração, bloqueio ou cancelamento de acessos a qualquer momento que julgar necessário.
4. Interceder junto à contratada quando for observado o mau uso do recurso de TIC e comunicar o fato ao Gestor do Recurso.
5. Solicitar o cancelamento do acesso ao término do contrato de serviço.

Das Unidades de TIC Descentralizadas

1. Garantir que as normativas internas estejam alinhadas com esta política e com as demais normativas relativas à Segurança da Informação e Comunicação da UFPR.
2. Informar à AGTIC, sempre que se fizer necessário, de medidas e ações que afetem o uso de recursos de TIC.

Da Direção Executiva da AGTIC

1. Divulgar periodicamente esta política por meio de canais oficiais da UFPR.
2. Fomentar o desenvolvimento de projetos que promovam a melhoria contínua nos controles de acesso e utilização dos Recursos de TIC.
3. Elaborar, divulgar e manter relação atualizada de softwares homologados para utilização nos computadores de rede.
4. Informar o SSIP de necessidades de atualização desta política sempre que se fizer necessário.

Do Subcomitê de Segurança da Informação e Privacidade

1. Manter esta política atualizada e alinhada com as necessidades institucionais e legais.
2. Aprovar e promover a presente Política no âmbito da UFPR.
3. Apreciar e aprovar alterações da Política.

DAS SANÇÕES DISCIPLINARES

Em casos comprovados de mau uso dos recursos de TIC, o acesso ao recurso poderá ser bloqueado ou cancelado e as informações sobre a infração serão fornecidas pelo Gestor do Recurso às autoridades responsáveis para que sejam tomadas as providências disciplinares previstas.

Curitiba, 18 de abril de 2023

Documento assinado eletronicamente por **RICARDO MARCELO FONSECA**, **REITOR**, em 18/04/2023, às 16:27, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida aqui informando o código verificador **5496950** e o código CRC **0A88EDD8**.