MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA
CAMPUS MINISTRO REIS VELLOSO

RESOLUÇÃO CONSUNI N° 63 DE 1º DE MARÇO DE 2024

Aprova e regulamenta a Política de Segurança da Informação e Comunicações no âmbito da Universidade Federal do Delta do Parnaíba

O REITOR DA UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA e PRESIDENTE DO CONSELHO UNIVERSITÁRIO - CONSUNI, no uso de suas atribuições, tendo em vista decisão do mesmo Conselho em reunião de 1º de fevereiro de 2024, e considerando:

- o Processo nº 23855.007381/2023-53

RESOLVE:

Art. 1º Regulamentar a Política de Segurança da Informação e Comunicação da Universidade Federal do Delta do Parnaíba, conforme disposto no anexo único desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação, conforme disposto no Parágrafo Único, do art. 4º, do Decreto nº 10.139, de 28 de novembro de 2019, justificando-se a urgência na excepcionalidade operacional da atividade administrativa da PROTIC/ UFDPar e a necessidade de sua regulamentação.

Vicente de Paula Censi Borges
Vice-Reitor, no exercício da Reitoria

ANEXO ÚNICO DA RESOLUÇÃO CONSUNI N° 63 DE 1º DE MARÇO DE 2024

CAPÍTULO I
DO ESCOPO

Art. 1º A Política de Segurança da Informação e Comunicação (PoSIC) é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico, gerencial e pelos usuários internos e externos a Universidade Federal do Delta do Parnaíba (UFDPar). A PoSIC tem o objetivo de garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações produzidas ou custodiadas pela UFDPar, em conformidade com 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.

§ 1º As diretrizes estabelecidas nesta política devem estar alinhadas ao Planejamento Estratégico Institucional, ao Plano Diretor de TI e Comunicação e em consonância com os valores institucionais.

§ 2º Integram também a PoSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

§ 3º As diretrizes, normas complementares e manuais de procedimentos da PoSIC da UFDPar se aplicam aos servidores docentes e técnico-administrativos, discentes, pesquisadores conveniados, prestadores de serviço, colaboradores, estagiários, consultores externos, relacionamento com outros órgãos públicos ou entidades privadas e a quem, de alguma forma, execute atividades vinculadas a esta Universidade.

§ 4º A PoSIC trata das diretrizes gerais acerca do uso e compartilhamento de ativos de informação durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade dos processos vitais da UFDPar, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, bem como os valores éticos e as melhores práticas de Segurança da Informação e das Comunicações (SIC).

§5º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pela UFDPar devem atender a esta PoSIC.

Art.2º A PoSIC estabelece diretrizes, normas, procedimentos, mecanismos, competências, responsabilidades, direcionamentos e valores a serem adotados para a Gestão de Segurança da Informação e Comunicações (GSIC) no âmbito da UFDPar, adequadas às responsabilidades, funcionalidades e peculiaridades de cada uma de suas áreas funcionais.

Art. 3º As diretrizes de Segurança da Informação e Comunicações (SIC) da UFDPar devem considerar, prioritariamente, seus processos, requisitos legais e sua estrutura.

Art. 4º A GSIC deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficácia e eficiência das atividades de SIC.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

Art. 5º Para efeitos desta PoSIC, adotam-se as seguintes conceituações:

I. **acesso:** possibilidade de consulta ou reprodução de documentos e arquivos;

II. **ameaça:** evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

III. **ativo:** qualquer bem, tangível ou intangível, que tenha valor para a organização;

IV. **ativo de informação:** ativo que guarda informações do órgão;

V. **autenticidade:** asseveração de que o dado ou a informação é verdadeiro e fidedigno tanto na origem quanto no destino;

VI. **cessão de bases de dados:** ato de disponibilizar cópia, total ou parcial, de dados da UFDPar, aprovada pelo gestor competente;

VII. **ciclo de vida da informação**: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua autenticidade, confidencialidade, integridade e disponibilidade;

VIII. **classificação:** atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

IX. **Comitê de Segurança da Informação e Comunicações:** grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da UFDPar;

X. **comprometimento:** perda de segurança resultante do acesso não-autorizado;

XI. **concedente:** responsável pelo fornecimento da base de dados confidenciais pela UFDPar;

XII. **confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

XIII. **conta de acesso:** conjunto do "nome de usuário" e "senha" utilizado para acesso aos sistemas informatizados e recursos de TIC;

XIV. **controles de segurança**: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XV. **credencial de segurança:** certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo;

XVI. **custodiante:** agente público responsável por zelar pelo armazenamento e pela preservação do ativo sob sua propriedade;

XVII. **dado:** informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XVIII. **dados confidenciais**: dados pessoais que permitam a identificação da pessoa e possam ser associados a outros dados referentes ao endereço, idade, raça, opiniões políticas e religiosas, crenças, ideologia, saúde física, saúde mental, vida sexual, registros policiais, assuntos familiares, profissão e outros que a lei assim o definir, não podendo ser divulgados ou utilizados para finalidade distinta da que motivou a estruturação do banco de dados, salvo por ordem judicial ou com anuência expressa do titular ou de seu representante legal;

XIX. **dados pessoais:** representação de fatos, juízos ou situações referentes a uma pessoa física ou jurídica, passível de ser captada, armazenada, processada ou transmitida por meios informatizados ou não;

XX. **disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

XXI. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR):** grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

XXII. **evento:** ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente conhecida que possa ser relevante para a segurança da informação;

XXIII. **gestor da informação:** agente público da UFDPar responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;

XXIV. **Gestor de Segurança da Informação e Comunicações:** é responsável pelas ações de segurança da informação e comunicações no âmbito da UFDPAR;

XXV. **grau de sigilo:** gradação de segurança atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;

XXVI. **incidente de segurança:** indício de fraude, sabotagem, desvio, falha, perda ou evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores;

XXVII. **informação custodiada:** informação sob a guarda e responsabilidade de alguém;

XXVIII. **integridade:** incolumidade de dados ou informações na origem, no trânsito ou no destino;

XXIX. **investigação para credenciamento:** averiguação sobre a existência dos requisitos indispensáveis para a concessão de credencial de segurança;

XXX. **legitimidade:** asseveração de que o emissor e o receptor de dados ou informações são legítimos e fidedignos tanto na origem quanto no destino;

XXXI. **marcação**: aposição de marca assinalando o grau de sigilo;

XXXII. **medidas especiais de segurança:** medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade, legitimidade e disponibilidade de dados e informações sigilosos. Também objetivam prevenir, detectar, anular e registrar ameaças reais ou potenciais a esses dados e informações;

XXXIII. **necessidade de conhecer:** condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança tenha acesso a dados ou informações sigilosas;

XXXIV. **ostensivo:** sem classificação, cujo acesso pode ser franqueado;

XXXV. **quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXVI. **reclassificação:** alteração, pela autoridade competente, da classificação de dados, informação, área ou instalação sigilosos;

XXXVII. **recursos de TIC:** recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XXXVIII. **rede corporativa:** conjunto de todas as redes locais sob a gestão da UFDPar;

XXXIX. **rede local:** conjunto de equipamentos interligados localmente com o objetivo de disponibilizar serviços aos usuários de rede da UFDPar;

XL. **segurança da informação:** proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

XLI. **senha ou palavra-chave:** é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo senhas amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema;

XLII. **sigilo:** segredo de conhecimento restrito a pessoas credenciadas e protegido contra revelação não autorizada;

XLIII. **software:** programa de computador desenvolvido para executar um conjunto de ações previamente definidas;

XLIV. **usuário da rede:** qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa da UFDPar;

XLV. **usuário de sistema**: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas disponibilizados pela UFDPar;

XLVI. **visita:** pessoa cuja entrada foi admitida, em caráter excepcional, em área sigilosa;

XLVII. **vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 6º Esta PoSIC e os documentos elaborados a partir dela devem obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

Art. 7º A PoSIC deve orientar-se pelos seguintes princípios da SIC: autenticidade, confidencialidade, disponibilidade, integridade e legalidade

CAPÍTULO IV
DAS DIRETRIZES

Seção I – Das Diretrizes Gerais

Art. 8º A UFDPar deve instituir uma estrutura organizacional estratégica de gestão de SIC, responsável pela execução dos processos de SIC.

§1º A estrutura deve definir um plano de SIC juntamente com um orçamento adequado para a implementação das ações definidas.

§2º A gestão de SIC deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as orientações estratégicas e necessidades operacionais prioritárias da autarquia e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

§3º A gestão de SIC deve continuamente orientar as melhores práticas e procedimentos de SIC, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

§4º A gestão de SIC deve assegurar que os usuários entendam suas responsabilidades e estejam de acordo com os seus papéis para prevenir fraudes, roubos ou mau uso dos recursos.

§5º A gestão de SIC deve manter continuamente a "equipe de prevenção, tratamento e resposta a incidentes cibernéticos, que comporá a rede de equipes dos órgãos e das entidades da administração pública federal, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República", conforme a redação dada pelo Decreto nº 10.641, de 2021.

§6º A gestão de SIC deve planejar a execução de programas, projetos e processos relativos a segurança da informação.

§7º A gestão de SIC deve priorizar a interoperabilidade de tecnologia, processos, informações e dados, com a promoção da integração e do compartilhamento dos ativos de informação do Governo federal ou daqueles sob sua custódia; com a uniformização e redução da fragmentação das bases de informação de interesse do Governo federal e da sociedade; com a integração e compartilhamento das redes de telecomunicações e da padronização da comunicação entre sistemas.

§8º A gestão de SIC deve estar sob o consentimento do proprietário da informação sigilosa recebida de outros países, nos casos de acordos internacionais.

§9º A gestão de SIC deve manter a cooperação entre os órgãos de investigação e os órgãos e as entidades públicas no processo de credenciamento de pessoas para o acesso às informações sigilosas.

§10 A gestão de SIC deve integrar e cooperar entre a UFDPar, o Poder Público, o setor empresarial, a sociedade, e a cooperação internacional, no campo da segurança da informação.

Art. 9º Os contratos firmados pela UFDPar devem conter cláusulas que determinem a observância desta PoSIC e seus respectivos documentos, bem como a manutenção do sigilo de suas informações durante e após sua vigência.

Art. 10 Os prestadores de serviços sob contrato com a UFDPar obrigatoriamente assinarão o Termo de Aceitação, em obediência ao estabelecido na PoSIC.

Art. 11 Para as diretrizes das seções abaixo, deve ser elaborada norma tática específica e Manual de Procedimentos.

Seção II – Do Tratamento da Informação

Art. 12 A UFDPar deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Seção III – Da Gestão de Incidentes

Art. 13 Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a impedir a interrupção das atividades e não afetar o alcance dos objetivos estratégicos.

Seção IV - Da Gestão de Risco

Art. 14 Deve ser estabelecido um processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) com vistas a minimizar possíveis impactos associados aos ativos, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança.

Seção V – Da Gestão de Continuidade

Art.15 Deve ser estabelecida a Gestão de Continuidade de Negócio no âmbito da UFDPar visando reduzir a possibilidade de interrupção causada por desastres ou falhas graves nos recursos que suportam as operações críticas desta Autarquia.

Seção VI – Da Auditoria e Conformidade

Art.16 O cumprimento desta PoSIC deve ser avaliado, periodicamente, pela alta direção, em conformidade com Normas Complementares, Manuais de Procedimentos e legislação específica de SIC, buscando a certificação do atendimento dos requisitos de segurança da informação. A alta direção poderá se valer de grupos internos ou externos para consecução de auditorias.

Seção VII – Do Controle de Acesso

Art.17 Devem ser instituídas normas que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação.

Seção VIII – Da Gestão de Operações e Comunicações

Art.18 Ações de segurança deverão garantir a operação segura e correta dos recursos de processamento da informação desta Autarquia.

Art.19 As atividades da UFDPar deverão ser protegidas contra interrupções não programadas.

Art. 20 O gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços.

Art.21 As informações e os recursos de processamento de informação deverão ter controles específicos que garantam a integridade e a disponibilidade dos mesmos.

Art. 22 As trocas de informações, tanto internamente, quanto externamente, deverão ser reguladas de forma a manter o nível adequado de segurança.

Art. 23 As operações deverão ser adequadamente monitoradas de forma a detectar atividades não autorizadas.

Seção IX – Da Segurança Física e do Ambiente

Art. 24 Os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência.

CAPÍTULO V
DAS PENALIDADES

Art. 25 Ações que violem qualquer dispositivo desta PoSIC, demais normas e procedimentos estabelecidos relativos a SIC, serão passíveis de investigação, podendo implicar em penas, sanções e penalidades previstas na legislação em vigor, em especial no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.117/2004 e na Lei nº 8.112/1990, que instituiu o Regime Jurídico dos Servidores Públicos Civis na União, das autarquias, inclusive as em regime especial, e das fundações públicas federais.

§1º No descumprimento previsto no caput por servidores, prestadores de serviços terceirizados, eventuais colaboradores ou estagiários, a UFDPar poderá determinar a respectiva substituição ou o desligamento, sem prejuízo das eventuais sanções penais e civis previstas na legislação aplicável (art. 116, inciso III, da Lei nº 8.112, de 1990).

§2º Os agentes públicos registrarão em Termo de Responsabilidade o conhecimento de todas as normas e procedimentos de SIC, bem como das penalidades a que estarão sujeitos em caso de descumprimento ou violação da PoSIC.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 26 É de responsabilidade de todos que têm acesso aos ativos da UFDPar manter níveis de segurança da informação adequados, segundo preceitos desta PoSIC.

Art. 27 É de responsabilidade da alta administração da UFDPar prover a orientação e o apoio necessários às ações de SIC, de acordo com os objetivos estratégicos e com as leis, regulamentos e normativas pertinentes.

Art. 28 Compete ao Gestor de Segurança da Informação e Comunicações da PROTIC:

I. promover cultura de segurança da informação e comunicações;

II. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. propor recursos necessários às ações de segurança da informação e comunicações;

IV. coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

V. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

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

VII. propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito da PROTIC;

VIII. coordenar a Gestão de Riscos de Segurança da Informação e Comunicações;

IX. coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;

X. prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR; e

XI. implementar procedimentos relativos ao uso dos recursos criptográficos, em conformidade com as orientações contidas na Norma Complementar 09/IN01/DSIC/GSIPR, de 22 de novembro de 2010.

Art.29 Compete ao Comitê de Segurança da Informação e Comunicações da UFDPar:

I. assessorar na implementação das ações de SIC na UFDPar;

II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

III. propor Normas e Procedimentos internos relativos à SIC em conformidade com as legislações sobre o tema;

IV. apurar incidentes que violem esta PoSIC; e

V. avaliar, revisar, analisar criticamente, propor alterações, dirimir eventuais dúvidas e deliberar sobre assuntos relativos a esta PoSIC e suas normas complementares, visando a sua aderência e concordância aos objetivos institucionais da UFDPar e às legislações vigentes.

Art. 30 Cabe ao Gestor do Ativo de Informação:

I. tratar e classificar a informação;

II. definir os requisitos de segurança para os ativos sob sua responsabilidade;

III. conceder e revogar acessos;

IV. autorizar a divulgação de informações.

Art. 31 Cada ativo de informação ou conjunto de ativos, dentro da UFDPar, deve ter um custodiante designado, pela autoridade competente da unidade administrativa, como o responsável por proteger e manter as informações e controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PoSIC.

Art. 32 Compete à Equipe de Segurança:

I. desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos da UFDPar;

II. avaliar, selecionar, utilizar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

III. conscientizar os usuários a respeito da implementação desses controles;

IV. verificar se todos os usuários colaboram com as medidas de segurança implantadas.

Art. 33 Cabe aos Gestores Administrativos:

I. multiplicar e catalisar os princípios de segurança;

II. autorizar concessão, transferência e revogação de acessos;

III. responder conjuntamente pelas ações realizadas por seus subordinados;

IV. conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

V. incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

VI. tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão.

Art. 34 É responsabilidade dos terceiros e fornecedores:

I. proteger os ativos de informação da UFDPar, incluindo informação, evitando perda ou modificação de dados, software e hardware;

II. assegurar o retorno ou a destruição da informação e dos ativos no final do contrato, ou em um dado momento definido no acordo;

III. observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade;

IV. observar restrições em relação à manutenção e instalação de software e hardware;

V. atender à política de controle de acesso desta Autarquia;

VI. relatar incidentes de segurança da informação e violação da segurança à equipe de segurança e à equipe de tratamento e respostas a incidentes; e

VII. atender aos princípios e diretrizes contidos nesta PoSIC, incluindo normas e procedimentos complementares destinados à SIC.

Art.35 É responsabilidade dos usuários:

I. difundir e exigir o cumprimento da PoSIC, das normas de segurança e da legislação vigente acerca do tema;

II. proteger os ativos de informação da UFDPar, incluindo informação, evitando perda ou modificação de dados, software e hardware;

III. observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade;

IV. observar restrições em relação à manutenção e instalação de software e hardware; V - atender à política de controle de acesso desta Autarquia;

V. relatar incidentes de segurança da informação e violação da segurança;

VI. atender aos princípios e diretrizes contidos nesta PoSIC, incluindo normas e procedimentos complementares destinados à SIC; e

VII. ser responsável por todos os atos praticados com suas identificações (login, crachá, carimbo, e-mail, assinatura digital, dentre outros).

CAPÍTULO VII
DA ATUALIZAÇÃO

Art. 36 Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser atualizados, sempre que se fizer necessário, com o objetivo de atender às exigências da legislação em vigor e/ou das transformações internas da UFDPar, não excedendo o período máximo de 03 (três) anos, conforme Norma Complementar 03/IN01/DSIC/GSIPR, de 30 de junho de 2009.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 37 Os casos omissos nesta Resolução serão direcionados ao Conselho Universitário - CONSUNI, pelo Comitê de Segurança da Informação da UFDPar.

Art. 38 Esta PoSIC entra em vigor na data de sua publicação.