UNIVERSIDADE FEDERAL DO OESTE DO PARÁ
CONSELHO SUPERIOR ADMINISTRAÇÃO

RESOLUÇÃO Nº 04 DE 20 DE OUTUBRO DE 2015.

Aprova a Política de Segurança da Informação e Comunicações no âmbito da Universidade Federal do Oeste do Pará.

O VICE-REITOR DA UNIVERSIDADE FEDERAL DO OESTE DO PARÁ, no uso de suas atribuições conferidas pela Portaria nº 817, de 10 de abril de 2014, publicada no diário oficial da União em 14 de abril de 2014, Seção 2, pág. 33, e consoante às disposições legais e estatutárias vigentes, em conformidade com os autos do Processo nº. 23204.004125/2015-11 proveniente do Centro de Tecnologia da Informação e Comunicação – Cetic e em cumprimento a decisão do egrégio Conselho Superior de Administração (CONSAD) na 3° Reunião Ordinária realizada no dia 17.09.15 promulga a seguinte:

RESOLUÇÃO

Art. 1º. Fica aprovada a Política de Segurança da Informação e Comunicações no âmbito da Universidade Federal do Oeste do Pará conforme documento em anexo (fls. 02/16).

Art. 2º. Esta Resolução entrará em vigor na data da sua publicação.

Prof. Dr. Anselmo Alencar Colares
Presidente
Conselho Superior de Administração

66

CAPÍTULO I
DO OBJETO

Art. 1º Fica estabelecida a Política de Segurança da Informação e Comunicações (POSIC), da Universidade Federal do Oeste do Pará (UFOPA), que estabelece as diretrizes de Segurança da Informação a serem observadas no âmbito desta Universidade.

§ 1º Documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

§ 2º A Política de Segurança da Informação e Comunicações da Universidade Federal do Oeste do Pará consiste na normatização de mecanismos que promovam a integridade da estrutura de rede e demais recursos de TIC nos quais trafegam informações e dados comuns ou restritos, neles incluídos os equipamentos que armazenam tais informações.

§ 3º São objetos da Política de Segurança, os serviços e recursos colocados à disposição dos servidores, estudantes, terceirizados e comunidade em geral, tais como: computadores, correio eletrônico, internet, informações armazenadas em diretórios da rede e sistemas de aplicação. As normas descritas no decorrer devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas e divulgadas, considerando-se o tempo hábil para que eventuais providências sejam tomadas. A aprovação das alterações será feita pelo Conselho Superior

Art. 2º A Política deve implementar controles para preservar os interesses dos servidores, estudantes, terceirizados e comunidade em geral contra danos que possam acontecer devido a falhas de segurança. Ela deve descrever as normas de utilização e possíveis atividades que possam ser consideradas como violação ao uso dos serviços, e, portanto, considerados proibidos.

§ 1º A Segurança da Informação estabelece um conjunto de políticas, normas e procedimentos que objetivam o controle de acesso, a preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade, integridade dos dados e responsabilidade das informações e dos recursos de TIC.

§ 2º Tais normas são fornecidas, a título de orientação aos servidores, estudantes, terceirizados e comunidade em geral. Em caso de dúvida o usuário deverá procurar a Coordenação de Segurança da Informação.

§ 3º A Coordenação de Segurança da Informação juntamente com o Comitê Gestor de Segurança da Informação é responsável por promover a cultura da segurança da informação apoiando e desenvolvendo atividades alinhadas com as estratégias de negócio da instituição a partir de um monitoramento contínuo dos seus processos, métodos e ações.

Art. 3º Caso os procedimentos ou normas aqui estabelecidos sejam violados, ao Comitê Gestor de Segurança da Informação se reserva o direito de propor as punições cabíveis aos usuários responsáveis pela violação da política com base em normas estabelecidas para este proposito. Esta política aplica-se a todos os usuários dos sistemas ou computadores da rede da UFOPA, sendo eles:

servidores, estudantes, trabalhadores terceirizados ou comunidade acadêmica em geral.

§ 1º O Comitê Gestor de Segurança da Informação é órgão responsável diretamente pela manutenção das políticas de segurança da informação na instituição.

§ 2º Cabe ao Comitê Gestor de Segurança da Informação propor normas e procedimentos relativos à Política de segurança da informação e Comunicação (POSIC), assim como assessorar na implementação das ações de segurança da informação e comunicação, sugerindo a criação de grupos de trabalho para tratar de temas e propor soluções específicas sobre a segurança da informação e comunicação.

Art. 4º A política aqui descrita, está dividida em política de segurança da estrutura de informática e política de segurança física. A primeira trata do acesso aos recursos computacionais e de rede, computadores, sistemas e correio eletrônico. A segunda aborda o acesso físico a sala de servidores ou ambientes especiais.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para fins de execução desta política, os ativos de TI serão definidos como qualquer bem, tangível ou intangível, que tenha valor para a instituição, classificados em:

I. Ativos de Informação: Sistemas de gestão de bancos de dados, documentos convencionais impressos ou em recursos digitais como *Cds, DVDs, pendrives, HDs* (internos e externos) e outras formas de armazenamento (disco, fitas. Etc.), além de qualquer recurso que faça parte dos sistemas de informação (SI) da instituição, dentre outros meios de geração de documentos que tenham valor para UFOPA;

II. Ativos de Sistemas: aplicações adquiridas pela UFOPA, softwares licenciados para instituição, aplicações desenvolvidas pela instituição, sistemas de gestão da instituição e todo patrimônio composto por dados e informações processadas por sistemas da UFOPA;

III. Ativos Físicos: equipamentos computacionais de grande e pequeno porte, equipamentos de comunicação, meios de entrada e saída como, impressoras, *scanner*, etc.

IV. Ativos de Infraestrutura: Sistemas de gerenciamento elétrico (geradores, *no breaks*, etc.), estruturas de redes (cabos, fibras, etc.), equipamentos de refrigeração, infraestrutura física, salas de aula, laboratórios, etc.

V. Incidentes de Segurança: É qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

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

Art. 6º Qualquer pessoa física ou jurídica com vínculo oficial com a UFOPA ou em condição autorizada que utiliza, de alguma forma, algum Recursos de Tecnologia da Informação e

Comunicação (RTIC) da UFOPA. Os usuários poderão ser cadastrados ou não no domínio da UFOPA e serão classificados, para fins de acesso aos recursos (RTIC), de acordo com os seguintes perfis:

I. Servidores: Todos os funcionários cadastrados como pertencentes ao quadro de força de trabalho desta instituição e registrados no setor de recursos humanos;

II. Alunos: Todos os graduandos e pós-graduandos que estiverem matriculados na UFOPA;

III. Outros: Qualquer pessoa com acesso autorizado aos serviços oferecidos pela instituição ou que estejam prestando algum tipo de serviço, como a comunidade em geral ou empresas terceirizadas, por exemplo.

Art. 7º Fazem parte do Princípios de Segurança da Informação:

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

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

III. Integridade: Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

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

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 8º Esta Política foi elaborada considerando o disposto em decretos e instruções normativas do governo federal:
I. Decreto nº 3.505, de 13 de junho de 2000, que institui a política de segurança da informação nos órgãos e nas entidades da Administração Pública Federal;

II. Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

III. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação o e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

IV. Instrução Normativa MPOG/SLTI nº 04/2010, que exige normas de segurança vigentes no órgão ou entidade e estabelece diretrizes para contratações de bens e serviços de TI;

IV. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para o credenciamento de segurança e tratamento da informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo Federal.

CAPÍTULO IV
DOS OBJETIVOS E DO ESCOPO

Art. 9º Fazem parte dos objetivos da POSIC/UFOPA:

I. Garantir que os recursos de informática e a informação serão utilizados de maneira adequada.

II. Orientar os usuários acerca das regras para utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar a Universidade Federal do Oeste do Pará, seus funcionários, alunos ou parceiros.

III. Incentivar o uso das soluções integradas de segurança;

IV. Servir de referência para auditorias, apuração e avaliação de responsabilidades.

§ 1º Os Recursos de Tecnologia da Informação e Comunicações (RTIC), abrangem os equipamentos, instalações e recursos de informação, direta ou indiretamente administrados, mantidos ou operados pelos usuários da instituição tais como:

I. Equipamentos de informática e telecomunicações de qualquer espécie;

II. Infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;

III. Laboratórios de informática de qualquer espécie;

IV. Recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação gerenciais, programas de computador, arquivos de configuração que são armazenados, executados e/ou transmitidos por meio da infraestrutura computacional da UFOPA, redes ou outros sistemas de informação.

§ 2º Os Serviços de Rede abrangem todos os serviços oferecidos aos usuários por meio da infraestrutura de rede interna e externa, tais como: correio eletrônico, *web sites* (páginas individuais e institucionais de conteúdos para a Internet), aplicações web (sistemas de uso da instituição acessados via rede), repositórios de arquivos em rede, servidores de bancos de dados individuais e corporativos, sistemas de autenticação de usuários de rede, serviços de segurança e monitoração, entre outros; bem como seus conteúdos (mensagens de correio eletrônico, dados corporativos, documentos, arquivos de configuração) que são hospedados e armazenados em máquinas servidoras sob a responsabilidade do CTIC.

§ 3º Os Sistemas de Informação abrangem os sistemas de controle, organização e planejamento acadêmicos e administrativos, bem como seus conteúdos hospedados e/ou armazenados em máquinas servidoras de responsabilidade do CTIC ou em máquinas locais com cópias de segurança em máquinas servidoras de responsabilidade do CTIC.

Art. 10 A Política de Segurança da Informação abrange os seguintes aspectos:

§ 1º Ficam estabelecidos os Requisitos de Segurança Lógica:

I. O acesso lógico a todos os ativos de informação da instituição devem ser controlados e protegidos;

II. Deve-se revisar periodicamente todas as autorizações de acesso e faz-se necessário registrar em *logs* os acessos afim de ser fazer auditoria em caso de ocorrência de algum fenômeno estranho que envolva os ativos de informação;

III. Deve-se adotar procedimentos de backup e recuperação de dados e fazer teste periódicos com o objetivo de manter a integridade e disponibilidade dos dados e aplicações, sendo necessário documentar todos os procedimentos e emitir relatórios periódicos dos testes;

IV. Deve-se proteger a infraestrutura de interligação lógica contra danos físicos e conexões não autorizadas.

§ 2º Ficam estabelecidos os Requisitos de Segurança Física:

I. Manter o sigilo sobre a localização da infraestrutura e os equipamentos que abrigam sistemas e guardam os dados críticos da instituição;

II. Controle de acesso a sala de servidores de dados e rede da instituição, devendo somente pessoal autorizado ter acesso a infraestrutura dos sistemas da instituição;

III. Fazer o registro da entrada e saída de pessoas a locais onde a segurança física e lógica guardam equipamentos e informações importantes para instituição, registrando local de acesso, data, hora e fazer a identificação das pessoas que estiverem em áreas de segurança;

IV. Sistemas de segurança para acesso físico deverão ser instalados para eventual controle de acesso de pessoas autorizadas e eventual auditoria.

§ 3º Ficam estabelecidos os Requisitos de Segurança em Recursos Humanos:

I. Combater erros humanos, prevenir fraudes e o uso não apropriado de senhas e recursos;

II. Treinamento de pessoal para prevenir eventuais crimes relacionados a engenharia social;

IV. Promover ações de combate a atividades ilícitas, conscientizando os recursos humanos da prevenção de vírus e aplicações maliciosas que possam comprometer a segurança dos ativos;

V. Avaliar criteriosamente o quadro funcional afim de delegar funções de confiança à pessoas que trabalharão com dados sigilosos, no intuito de preservar informações confidencias;

VI. Verificar o histórico de vida pública do funcionário com objetivo de certifica-se que o mesmo está apto a ter acesso a informações sensíveis;

V. Proteger as informações da instituição de modo a não guardar dados institucionais na nuvem;

VI. Habilitar os usuários por meio de credencial que indique que ele está autorizado a desenvolver determinada função de acordo com seu cargo e grau de sigilo. E que está autorizado a acessar determinadas informações ou locais considerados restritos.

§ 4º Ficam estabelecidos os Requisitos de Segurança dos Recursos Criptográficos.

I. O sistema de chaves criptográficas deve ser avaliado anualmente por especialistas da área afim de manter a segurança dos ativos que compõem a informação;

II. Manter sigilo das chaves criptográficas e das senhas administrativas dos sistemas da instituição;

III. A utilização das chaves criptográficas deve ser restrita a um determinado número mínimo e essencial de pessoas autorizadas, com competência para gerir os sistemas criptográficos da instituição;
IV. Como qualquer outro ativo considerado crítico para instituição, os recursos criptográficos devem ser mantidos sob segurança física e lógica.

§ 5º A Política de Segurança é constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pela UFOPA.

§ 6º A POSIC/UFOPA é aplicável a todos os bens e serviços e a todo o pessoal que se utiliza dos recursos de Tecnologia da Informação e Comunicação (TIC), no âmbito da UFOPA.

§ 7º Serão elaboradas pela Coordenação de Segurança da Informação normas especificas, baseadas em padrão ABNT, que estabelecerão as responsabilidades sobre os ativos de TI e os requisitos de segurança, submetendo-as ao Comitê Gestor de Segurança da Informação para homologação e aprovação final pelo Conselho Superior/UFOPA.

CAPÍTULO V
DO GERENCIAMENTO DE RISCOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 11 Entende-se como gerenciamento de riscos o processo que visa à proteção dos serviços da UFOPA, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser identificados:

I. O que deve ser protegido (Ativos):

a) Equipamentos considerados críticos precisam estar instalados em áreas protegidas e gerenciadas por controles de acessos;

b) Proteção adequada do cabeamento elétrico e da rede lógica que alimenta e interliga todos os equipamentos;

c) A manutenção preventiva dos equipamentos deve ser feita conforme as especificações do fabricante.

II. Análise de riscos (contra quem ou contra o quê deve ser protegido):

a) Equipamentos com custo financeiro elevado considerados de difícil reposição, precisam estar seguros contra ameaça de incêndio;

b) Proteger os equipamentos e informações contra o risco de ameaças externas e do meio ambiente, assim como falhas humanas;

c) Zelar pela segurança das instalações prediais que ao menos devem estar protegidas contra incêndio;

d) Criar mecanismos de proteção e combate a incêndio, principalmente em locais considerados críticos.

III. Avaliação de riscos (análise da relação custo/benefício):

a) Colocar em operação um gerador próprio e um sistema de no-break, com o proposito de alimentar pelo menos os equipamentos considerados mais críticos, diminuindo os riscos dos sistemas de informação ficarem indisponíveis por falhas elétricas e protegendo os dados de serem corrompidos;

b) Planejamento para a implantação de sistemas de controle local de condições ambientais a fim de garantir que equipamentos considerados críticos não sofram falhas por questões de temperatura.

§ 1º A Coordenação de Segurança da Informação apresentará planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Comitê Gestor de Segurança da Informação e executados pela Coordenação de Segurança da Informação (CSI) e demais coordenações do Centro de Tecnologia da Informação (CTIC).

§ 2º As normas e procedimentos para implantação e gerenciamento de riscos de Informação serão definidos em documento específico elaborado pela CSI/CTIC/UFOPA e aprovado pelo Comitê Gestor de Segurança da Informação.

§ 3º A UFOPA deverá realizar treinamentos específicos de conscientização para todos os servidores em noções de segurança da informação visando à implantação e gerenciamento de todos os componentes do Sistema de Gestão de Segurança da Informação (SGSI) e a agilidade da notificação de qualquer evento relacionado a segurança da informação que venha a ocorrer.

Art. 12 Será criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR que ficará responsável por receber, analisar, classificar e responder as notificações relacionadas aos incidentes de segurança em redes de computadores. Os incidentes serão filtrados e classificados quanto ao nível de ameaça para que as mesmas sejam prevenidas e eliminadas, afim de proteger a rede de possíveis atividades maliciosas.

§ 1º Tratamento de Incidentes em Redes Computacionais é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

I. Incidentes de Segurança:

a) Qualquer evento que ameace a integridade , confidencialidade, disponibilidade e autenticidade das informações;

b) Qualquer ocorrência que venha a descumprir as regras da Política de Segurança da Informação e Comunicação e demais políticas que estejam relacionadas a segurança dos recursos de tecnologia da informação.

§ 2º Deverão ser realizados procedimentos de tratamento, armazenamento, identificação e classificação das informações da Universidade de tal forma a garantir a integridade, facilidade de localização e evitar o uso dessas informações por pessoas não autorizadas.

§ 3º O descarte de informações sensíveis deverá ser realizado através de trituração, incineração ou remoção dos dados de forma segura.

§ 4º Deverão ser realizadas cópias de segurança (backup) das informações tomando como base a norma de gerenciamento de cópias de segurança da informação da UFOPA.

§ 5º As cópias de segurança das informações deverão ser testadas, verificadas e armazenadas, local e remotamente, de tal forma a evitar a perda da informação por alguma eventualidade.

CAPÍTULO VI
DO PLANO DE CONTINUIDADE DE NEGÓCIOS

Art. 13 O Plano de Continuidade de Negócio (PCN) tem como objetivo manter em funcionamento os serviços e processos críticos da UFOPA na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, falhas humanas e qualquer outro tipo de eventualidade que venha a ocorrer.

I. Os planos de continuidades devem prever as seguintes eventualidades:

a) em caso de perda total do prédio;

b) em situações que afetem áreas críticas;

c) perda total dos equipamentos que fornecem energia elétrica (geradores, transformadores, estações de energia, sistemas de *no-break*, etc);

d) perda de servidores de rede – arquivos, comunicação e aplicações;

e) perda de equipamentos de comunicação de dados (controladoras de comunicação, roteadores, *switchs*, *modens*, linhas, cabos e etc.);

f) perda de unidades de discos consideradas críticas;

g) perda do sistema de I/O em fita;

h) perda de impressoras consideradas críticas;

i) parada de sistemas considerados críticos (sistema de comunicações de dados, sistemas gerenciadores de bancos de dados, sistemas de atendimento ao público, sistema financeiros, sistemas de gerenciamento de recursos humanos, sistemas de gerenciamento acadêmico etc.); e

j) greve de pessoal.

§ 1º Os planos de continuidade devem passar por validações periódicas afim de encontrar falhas que possam a vir ocorrer na elaboração de determinado plano, as falhas devem ser documentadas e os planos corrigidos.

§ 2º O PCN da UFOPA será definido pelo Centro de Tecnologia da Informação com base na análise de riscos e terá a homologação do Comitê Gestor de Tecnologia da Informação e posterior aprovação do CONSUN/UFOPA.

CAPÍTULO VII
DAS AUDITORIAS E FISCALIZAÇÕES

Art. 14 Todos os usuários estão sujeitos à auditoria em sua utilização dos recursos (RTIC). Os procedimentos de auditoria e de monitoramento de uso dos recursos (RTIC) serão realizados periodicamente pela Coordenação de Segurança da Informação e demais coordenações do CTIC o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança.

Art. 15 Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja a POSIC e normas complementares, será permitido à Coordenação de Segurança e Demais Coordenações do CTIC auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário e ao Diretor do CTIC e/ou ao presidente do Comitê Gestor de Segurança

da Informação da UFOPA dependendo da gravidade.

Parágrafo Único. Será considerada gravidade baixa a atividade que comprometa apenas a máquina do usuário, gravidade média a atividade que comprometa o desempenho da rede e gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços.

CAPÍTULO VIII
DO CONTROLE DE ACESSO E DA UTILIZAÇÃO DOS RECURSOS DE TI

Art. 16 Todos os usuários da UFOPA têm o direito ao uso dos recursos (RTIC) da UFOPA de acordo com as diretrizes de seu perfil, definidas por meio de requisitos técnicos ou por determinação específica da Reitoria ou dos órgãos da administração superior.

Art. 17 Por medida de segurança somente os técnicos do CTIC e do setor de SUPORTE devem possuir privilégios de administrador nos computadores da instituição, isso evita que os usuários comuns instalem softwares piratas nos sistemas operacionais e evita também que sejam instalados softwares maliciosos que possam prejudicar os computadores da instituição e colocar em risco a segurança das informações institucionais.

Art. 18 Ficam assim, estabelecidas regras para controle de acesso e utilização dos recursos de TI:

I. Somente os técnicos do SUPORTE estão autorizados a instalar quaisquer programas para atender a necessidade dos usuários desde que estes sejam licenciados ou gratuitos.

II. Não são permitidos em hipótese alguma a instalação de Softwares sem licença de uso ou que apresentem algum risco ao computador ou ao funcionamento da rede da instituição;

III. Fica vedado o uso de recursos da rede para atividades que comprometam o desempenho da mesma, tais como uso de aceleradores de download, baixar filmes e vídeos que não sejam para uso institucional ou acadêmico;

IV. O acesso aos serviços de rede da UFOPA que necessitam autenticação só será permitido a usuários cadastrados;

V. O acesso aos recursos (RTIC) será feito por controles físicos ou lógicos, com objetivo de proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

Art. 19 Serão estabelecidas normas para o acesso de pessoas que não fazem parte da comunidade acadêmica e serão definidos mecanismos de controle para a identificação das mesmas, registrando o acesso por meio da data, hora e quem autorizou o acesso, afim de diminuir os riscos e facilitar a auditoria de eventos que possam trazer riscos a segurança da informação.

Art. 20 Quando da utilização de nome de usuário e senha, estes serão definidos no momento de ingresso na UFOPA.

Art. 21 Todos os usuários deverão por meio de um termo de responsabilidade específico assumir o

compromisso de:

I. Declarar o conhecimento e aceitação dos termos desta política de segurança e de suas políticas e normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

II. Declarar estar ciente que os acessos realizados à Internet, assim como conteúdo das mensagens de correio eletrônico institucional são passíveis de auditoria.

Art. 22 Qualquer tipo de informação referente a conteúdos que dizem respeito à instituição deverão ser guardados em lugar seguro como, por exemplo, cofres, armários e mobílias que possuam algum tipo de fechadura quando não estiverem em uso.

Art. 23 Qualquer tipo de equipamento de armazenagem e processamento de informação com tombamento (Ex.: estações de trabalho, notebooks, celulares) só poderão ser utilizados fora das dependências do instituto ou do setor de sua responsabilidade com autorização prévia e protegido de forma adequada contra furto, roubo ou perda da informação.

Art. 24 É de total responsabilidade do usuário a proteção das informações institucionais que estejam sob sua responsabilidade, utilizadas no âmbito do instituto ou fora de suas dependências.

Art. 25 Os usuários devem seguir a politica de tela limpa e mesa limpa, evitando que informações confidencias ou restritas estejam ao alcance de pessoas não autorizadas.

I. A política de tela limpa define um bloqueio automático do computador quando um usuário se ausentar do mesmo por um determinado tempo configurado. Isto evita o acesso indevido ao computador por pessoas não autorizadas durante a ausência do servidor ou usuário autorizado.

II. A política de mesa limpa define que documentos e carimbos não devem ser mantidos na mesa do usuário ao fim do expediente ou em caso de ausência prolongada.

Parágrafo Único. O gerenciamento de informações, documentos e materiais sigilosos da UFOPA deverão estar em conformidade com a Lei no 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e com o Decreto no 4.553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

CAPÍTULO IX
DOS SERVIÇOS DE CORREIO ELETRÔNICO

Art. 26 Os serviços de correio eletrônico hospedados em máquinas servidoras da UFOPA são oferecidos como um recurso profissional para apoiar os usuários cadastrados da Universidade no cumprimento dos objetivos institucionais e são passíveis de auditoria.

Art. 27 Os serviços de correio eletrônico deverão garantir o sigilo, a confidencialidade, o não-repúdio, a autenticidade, a disponibilidade geral do serviço e, os usuários que o utilizarem, deverão assegurar que o endereçamento da mensagem esteja correto.

Art. 28 O usuário compromete-se a utilizar o serviço de correio eletrônico de acordo com a legislação vigente e com as condições desta politica de segurança, assim como as demais regras especificas que regem o serviço de correio eletrônico da instituição. As regras para utilização do e-mail institucional estão descritas abaixo:

I. Verificar regularmente a caixa de entrada do e-mail institucional sempre que o servidor estiver no seu ambiente de trabalho. Ao terminar suas atividades o servidor deverá encerrar sua sessão para que outras pessoas não tenham acesso indevido ao e-mail;

II. As mensagens do e-mail devem ser acessadas somente por seus remetentes e destinatários, são confidenciais e devem ser preservadas para que não sejam lidas por pessoas não autorizadas;

III. As mensagens lidas e sem grande importância devem ser apagadas com proposito de não exceder o limite da caixa postal, ficando salvas as mensagens que o servidor considere de extrema importância para se respaldar, se preciso, por meio de uma mensagem que comprove eventos praticados via e-mail (comprovação de serviços, pedidos feitos via e-mail, e-mail que comprove outros tipos de atividades, etc.);

IV. Devem ser veiculadas via e-mail institucional somente mensagens com conteúdo de interesse acadêmico ou administrativo, não sendo permitido a utilização para fins comerciais, uso politico, manifestação religiosa, spam, pornografia, correntes eletrônicas e demais conteúdos que não sejam de interesse da instituição;

V. O e-mail não poderá ser ser utilizado para publicação de qualquer tipo de conteúdo relacionado a discriminação e que incentive a violência em relação a uma pessoa ou grupo de pessoas por conta da raça, credo, opção sexual ou nacionalidade;

VI. O usuário do e-mail institucional deve ter cuidado para que não sejam modificados arquivos sem autorização, e para que outras pessoas não assumam suas identidades enviando e-mail com a identificação do titular da conta. O e-mail é de uso particular e sempre deverá ser utilizado pelo titular, ficando proibido o repasse de senhas;

VII. Não é permitido o envio de arquivos que contenham vírus, softwares maliciosos, arquivos corrompidos ou quaisquer outras aplicações que possam vir danificar os computadores da instituição e o tráfego da rede;

IX. O uso do correio eletrônico da instituição não deverá ser utilizado para o envio e recebimento de mensagens pessoais individuais que não sejam de interesse acadêmico ou administrativo, sendo considerado inadmissível que usuário faça cadastro com e-mail institucional em sites de compras, promoções, redes sociais e outras atividades não relacionadas ao interesse da UFOPA;
X. Fica vedada a distribuição da lista de endereços dos usuários do e-mail institucional a qualquer pessoa estranha que não seja do quadro de servidores da UFOPA, salvo em casos de interesse institucional;

XI. Não é permitido redirecionamento de e-mail institucional para caixas de e-mail particulares com a intenção de obter mais espaço.

Parágrafo Único. Caso venham acontecer ocorrências que ponham em risco a segurança do e-mail institucional, será feito um trabalho de auditória para apurar os fatos e reserva-se ao Comitê Gestor de Segurança da Informação o direito de julgar tais fatos com o intuito de punir os infratores das normas de utilização do e-mail da instituição.

CAPÍTULO X
DA PUBLICAÇÃO E DO ACESSO À INTERNET

Art. 29 Toda informação publicada no sitio oficial da UFOPA será de responsabilidade do usuário que realizou a publicação.

Art. 30 Toda comunidade acadêmica têm o direito de acesso à internet, conforme as permissões de acesso estipuladas nas normas de segurança da instituição. Esse acesso deverá ser feito exclusivamente para fins diretos e complementares às atividades da instituição, para o enriquecimento intelectual de seu corpo discente, docente, técnico e demais categorias ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

CAPÍTULO XI
DOS DEVERES E DAS RESPONSABILIDADES

Art. 31 É dever de todo usuário dos ativos de TI da UFOPA:

I. Conhecer a POSIC e manter níveis de segurança adequados, seguindo as suas diretrizes e normas complementares.

II. Adotar comportamento seguro, assumindo atitude pró-ativa e engajada no que diz respeito à proteção das informações da Universidade.

III. Os mesmos devem manter a confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério do CTIC.

Art. 32 Os institutos e Pró-reitorias são responsáveis pela garantia da segurança das informações acadêmicas no âmbito da UFOPA, ressalvadas as situações em que:

I. A informação for retirada do âmbito da rede da UFOPA por usuários autorizados;

II. O usuário autorizado fornecer sua senha de acesso a qualquer outra pessoa;

III. O acesso à informação for limitado ou não disponibilizado por serviços e estruturas externas a UFOPA ou de responsabilidade de outros órgãos ou terceiros;

IV. quando propositadamente ou inadvertidamente o usuário fizer uso inadequado dos recursos (RTIC), seja por inabilidade, conhecimento insuficiente ou intenção de causar dano à instituição ou a outrem.

Art. 33 Caberá a Diretoria de Gestão e Desenvolvimento de Pessoas:

I. Desenvolver juntamente com os gestores de segurança da informação o termo ou termos de responsabilidade que incluam regras quanto ao uso dos recursos de TI, ativos de informação e quanto ao sigilo das informações da instituição;

II. Obter a assinatura do Termo de Responsabilidade e informar à equipe de Tecnologia da Informação sobre mudanças no quadro funcional da Instituição.

Art. 34 Cabe a Coordenação de Segurança da Informação a tarefa de:

I. Elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicações (POSIC) e normas relacionadas, submetendo a aprovação do Comitê Gestor de Segurança da Informação;

II. Propor, acompanhar e divulgar os planos de ação para aplicação da POSIC, incluindo a conscientização de usuários;

III. Propor a implantação de soluções para minimização dos riscos que visem à segurança dos ativos de informação da UFOPA;

IV. Elaborar propostas de normas complementares e políticas de uso dos recursos de informação;

V. Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação;

VI. Fazer o alinhamento estratégico com as diretrizes da instituição;

VII. Apontar investimentos necessários com intuito de reduzir os riscos relacionados à segurança da informação.

Art. 35 Caberá a Equipe de Tratamento e Respostas a Incidentes Computacionais (ETIR) analisar e responder às notificações e monitorar as atividades relacionadas a incidentes de segurança em redes de computadores.

Art. 36 Os gestores terão a responsabilidade de zelar pelo cumprimento das diretrizes da POSIC.

CAPÍTULO XII
DAS SANÇÕES E PENALIDADES

Art. 37 A quem descumprir esta política de segurança, as normas e procedimentos estabelecidos pela UFOPA serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

I. Na Lei no 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;

II. No Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto no 1.171/1994;
III. No Código Penal, através do Decreto-Lei no 2848/1940;

IV. Na Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

IV. No Decreto no 4553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

CAPÍTULO XIII
DAS DISPOSIÇÕES FINAIS

Art. 38 Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicação da UFOPA, devem ser direcionados a Coordenação de Segurança da Informação, com a interveniência do Comitê Gestor de Tecnologia da Informação.

Art. 39 A POSIC e suas atualizações deverão ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados que habitualmente trabalham na UFOPA.

Art. 40 Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 01 (um) ano.

Art. 41 A POSIC da UFOPA se aplica a todos os integrantes do quadro de funcionários, discentes, terceirizados que estejam prestando serviços para a instituição e a toda comunidade em geral que de alguma forma esteja utilizando os recursos de TI da UFOPA. Além dos recursos administrativos e tecnológicos, abrange os recursos ligados a esta Universidade em caráter permanente ou temporário.

Art. 42 Serão criadas normas complementares a este documento com o objetivo de estabelecer regras especificas para a utilização de recursos, acesso a ambientes de segurança, serviços, etc.

CAPÍTULO XIV
DA VIGÊNCIA

Art. 43 A presente política passa a vigorar a partir da data de sua publicação.