UNIVERSIDADE FEDERAL DO OESTE DO PARÁ
CONSELHO SUPERIOR DE ADMINISTRAÇÃO

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
COORDENAÇÃO DE SISTEMAS

NORMAS PARA GERENCIAMENTO, PRODUÇÃO E USO DE SISTEMAS DE INFORMAÇÃO

CAPÍTULO I
DO OBJETIVO

Art. 1º Estabelecer as responsabilidades e regras para o desenvolvimento, administração e uso de sistemas de informação da instituição.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 2º Este documento se aplica aos profissionais que gerenciam e desenvolvem sistemas de informação, a todos os usuários que utilizam os sistemas desenvolvidos e mantidos por esta instituição e está alinhado com a Política de Segurança da Informação da UFOPA.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Define termos referentes à tecnologia da informação e segurança da informação:
I – Política de Segurança da Informação: Documento que estabelece diretrizes de Segurança da Informação a serem observadas no âmbito da Universidade Federal do Oeste do Pará;
II – ativos: Tudo aquilo que tem valor para universidade, sejam equipamentos, softwares ou pessoas. Tudo aquilo que necessita de proteção;
III – incidentes de segurança: É qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança da informação;
IV – requisição: É qualquer solicitação, contato, pedido de informação ou dúvida para acessar um serviço, e geralmente não requer uma requisição de mudança;
V – sistemas de informação: Elementos que fazem parte de um conjunto organizado, podendo ser pessoas, dados, atividades e/ou recursos físicos ou lógicos;
VI – software: Conjunto de instruções que comandam operações feitas por um computador.

CAPÍTULO IV
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4º Esta norma se baseia nas diretrizes estabelecidas pelo Art. 1º da Resolução nº 04 de 20 de outubro de 2015, que aprova a Política de Segurança da Informação e Comunicações no âmbito da Universidade Federal do Oeste do Pará.

CAPÍTULO V
DOS DEVERES E RESPONSABILIDADES DA INSTITUIÇÃO

Art. 5º A instituição compromete-se a manter a privacidade dos usuários e compromete-se com a proteção de dados pessoais sob sua custódia e controle.

Art. 6º Cabe à Universidade Federal do Oeste do Pará, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
I – gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação no que consiste em domínio público;
II – proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade;
III – proteção das informações sigilosas e das informações relativas ao ambiente de trabalho, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso;
IV – manutenção da infraestrutura necessária para que os sistemas de informação da universidade estejam sempre disponíveis.

Art. 7º Os dados pessoais sob responsabilidade da instituição devem estar protegidos de acessos não autorizados seguindo normas e procedimentos, mantendo o uso seguro dos sistemas de informação.

CAPÍTULO VI
DOS DEVERES E RESPONSABILIDADES DOS USUÁRIOS

Art. 8º O usuário compromete-se a obedecer às políticas e normas referentes a segurança da informação.

Art. 9º Os usuários devem seguir políticas de alteração de senhas sempre que suspeitar de irregularidades e sempre que for solicitado a executar esta tarefa via sistemas:
I – deve-se estabelecer um período máximo para troca da senha;
II – o usuário poderá efetuar a troca da sua senha a qualquer momento;
III – será estabelecido um número mínimo de caracteres para o tamanho da senha;
IV – não será permitido a solicitação de senha de um usuário por outro usuário, mesmo em situação de chefia e subordinado;
V – o processo de gerenciamento de senhas deve adotar criptografia das mesmas;
VI – o compartilhamento de login e senhas fere a política de segurança da informação;
VII – é dever de qualquer usuário informar sobre falhas e vulnerabilidades encontradas em sistemas de informação da instituição;
VIII – o usuário que se aproveitar de falhas encontradas em sistemas e fizer o uso mal intencionado das mesmas, poderá sofrer Processo Administrativo por tentar lesar a instituição.

CAPÍTULO VII
DO PROCESSO DE DESENVOLVIMENTO DE SISTEMAS

Art. 10 É necessário que se adotem normas e procedimentos de segurança no processo de gerenciamento e desenvolvimento de sistemas de informação:
I – dividir o ambiente de desenvolvimento de sistemas em ambiente de homologação e produção, testando os softwares antes de serem colocados em produção, separando os ambientes de desenvolvimento, teste e produção;
II – os servidores de banco de dados devem ser gerenciados de forma que sejam acessados apenas por usuários autorizados;

III – o processo de desenvolvimento de softwares deve adotar metodologias que envolvam a segurança da informação, a fim de manter sistemas seguros e menos vulneráveis a falhas e quebras de segurança;
IV – desenvolver softwares fechando brechas de segurança;
VI – manter a infraestrutura de desenvolvimento sempre atualizada;
VII – documentar todo processo de desenvolvimento e atualização de software;
VIII – manter cópias de segurança dos sistemas.

Art. 11 Problemas ou demandas relacionadas a sistemas de informação serão atendidos via sistema de abertura de chamado, memorandos eletrônicos e quando necessário, através de processo.

Art. 12 O desenvolvimento de novos sistemas deverá ser precedido de análise, verificando-se as necessidades da aplicação e se os sistemas institucionais existentes não contemplam, além da viabilidade do projeto.
Parágrafo único. A equipe de desenvolvimento de software poderá fornecer treinamento aos usuários de sistemas sempre que for necessário.

Art. 13 A Coordenação de Sistema é responsável por elaborar e definir procedimentos de desenvolvimento de sistemas e sites que deverão ser respeitados pelos solicitantes.

CAPÍTULO VIII
DO DESENVOLVIMENTO E GERENCIAMENTO DE SITES

Art. 14 O desenvolvimento de site é restrito apenas para fins institucionais.

Art. 15 A inserção de conteúdo em site institucional fica restrito ao que diz a politica de conteúdo e os responsáveis.

Art. 16 Sites desenvolvidos por terceiros, quando da integração com a infraestrutura já montada, deverão adequar-se para o perfeito funcionamento.

Art. 17 Não é responsabilidade da Coordenação de Sistemas promover a atualização técnica de sites desenvolvidos por terceiros e integrados à instituição.

Art. 18 Deve-se manter monitoramento contínuo sobre as aplicações e web sites, verificando falhas e ameaças.

CAPÍTULO IX
DA AUDITORIA DOS SISTEMAS

Art. 19 Os sistemas de informação da instituição estão sujeitos à auditoria sempre que for necessário, tanto para avaliar os aspectos de sua segurança, quanto para apurar incidentes.

Art. 20 Todas as tentativas de logon serão registradas em arquivos de logs.

Art. 21 As informações disponibilizadas nos sistemas e meios de informação da instituição são responsabilidades de quem as inseriu.

Parágrafo Único. Softwares, sistemas administrativos e acadêmicos fazem parte da infraestrutura de sistemas de informação da instituição.

CAPÍTULO X
SISTEMA INTEGRADO DE RECURSOS HUMANOS
SIGRH

Art. 22 Sistema adotado pela instituição para o controle e gerenciamento dos recursos humanos:
I – a unidade de gestão de recursos humanos é a responsável principal pela utilização do referido sistema;
II – a atualização de informações, exceto aquelas que o próprio servidor público não pode realizar dentro dos limites que o sistema estabelece, deverá ser realizada pela unidade gestora de recursos humanos;
III – a solicitação de perfil de acesso a determinada funcionalidade do sistema deve ser precedida de solicitação formal do chefe da unidade requisitante e aprovada pela unidade responsável pela utilização do referido sistema;
IV – com vistas à segurança, o perfil solicitado terá duração de 01 ano, podendo ser prorrogado a pedido do chefe da unidade por igual período conforme a conveniência;
V – a implantação de novo módulo, deve estar de acordo com o planejamento do ano corrente da instituição e formalmente aprovado pela Pró-reitoria de Planejamento.

Parágrafo único. Os sistemas administrativos e acadêmicos estão implantados para fornecer o apoio necessário as atividades desenvolvidas pela universidade. São gerenciados por usuários com privilégios administrativos e cada sistema tem suas regras.

CAPÍTULO XI
SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS
SIPAC

Art. 23 Sistema adotado pela instituição para o gerenciamento e controle das atividades administrativas.
I – a Pró-reitoria de Planejamento e a Pró-reitoria de Administração são as responsáveis principais pela utilização do referido sistema;
II – a solicitação de perfil de acesso a determinada funcionalidade do sistema, deve ser precedida de solicitação formal do chefe da unidade requisitante e aprovada pela unidade responsável pela utilização do referido sistema;
III – com vistas à segurança, o perfil solicitado terá duração de 01 ano, podendo ser prorrogado a pedido do chefe da unidade por igual período conforme a conveniência;
IV – a implantação de novo módulo, deve estar de acordo com o planejamento do ano corrente da instituição e formalmente aprovado pela Pró-reitoria de Planejamento.

CAPÍTULO XII
SISTEMA INTEGRADO DE GESTÃO DE ATIVIDADES ACADÊMICAS

SIGAA

Art. 24 Sistema adotado pela instituição para o gerenciamento e controle das atividades acadêmicas.
I – a Pró-reitoria de Ensino e Graduação, a Pró-reitoria de Pesquisa e Inovação Tecnológica, a Ouvidoria, a Comissão Própria de Avaliação, e a Biblioteca são as responsáveis principais pela utilização do referido sistema;
II – a solicitação de perfil de acesso a determinada funcionalidade do sistema, deve ser precedida de solicitação formal do chefe da unidade requisitante e aprovada pela unidade responsável pela utilização do referido sistema;
III – com vistas à segurança, o perfil solicitado terá duração de 01 ano, podendo ser prorrogado a pedido do chefe da unidade por igual período conforme a conveniência;
IV – a implantação de novo módulo, deve estar de acordo com o planejamento do ano corrente da instituição e formalmente aprovado pela Pró-reitoria de Planejamento.

CAPÍTULO XIII
DA VIGÊNCIA

Art. 25 Estas normas passam a vigorar a partir da data de sua aprovação pelo Conselho Superior desta instituição.