POLÍTICA DE SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DA SOHIDRA

1. APRESENTAÇÃO

A presente Norma tem como base o Dec. 29.227, de Segurança da Informação do Governo do Estado do Ceará, de 13 de março de 2008. Ressalta-se que serviços e recursos computacionais oferecidos pela SOHIDRA impõem responsabilidades e obrigações a seus usuários, com o objetivo de criar uma ética de utilização e compartilhamento desses serviços e recursos, preservar a propriedade intelectual e os direitos sobre dados, manter a integridade da segurança dos sistemas e evitar intimidações, embaraços e aborrecimentos desnecessários. Considerando que o uso dos serviços de informação, não só na SOHIDRA, como no âmbito do Governo do Estado do Ceará, é uma concessão e não um direito. É de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada dos recursos tecnológicos.

2. ABRANGÊNCIA

Esta norma deverá ser aplicada a todos os colaboradores que possuam acesso às pastas e servidores da SOHIDRA, sistemas internos e externos computacionais do Governo do Estado do Ceará.

3. VIGÊNCIA

Esta Norma passa a vigorar a partir da data de sua aprovação e será revisada anualmente. A antecipação do processo de revisão poderá ocorrer pela necessidade de reestruturação dos processos administrativos/operacionais da SOHIDRA.

4. PROCEDIMENTOS

Todos os procedimentos devem observar as normas contidas no Dec. 29.227 de 13 de março de 2008, que DISPÕE SOBRE A INSTITUIÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - TIC DO GOVERNO DO ESTADO DO CEARÁ E DO COMITÊGESTOR DE SEGURANÇA DA INFORMAÇÃO DO GOVERNO DO ESTADO DO CEARÁ– CGSI.

Segue as normas, conforme Decreto citado:

a) Norma NPS01 – Uso do Correio Eletrônico – (e-mail);
b) Norma NPS02 – Uso da Internet;
c) Norma NPS03 – Criação de Contas e Senhas de Usuários;
d) Norma NPS04 – Criação de Contas e Senhas para Administradores;
e) Norma NPS05 – Gestão de Ativos;
f) Norma NPS06 - Contingência e Continuidade do Negócio.

5. DA UTILIZAÇÃO

Utilizar os serviços e recursos somente para as necessidades autorizadas, tais como, desenvolvimento de trabalhos administrativos, financeiros, gerenciais e afins. Proteger sua identificação de usuário e sua senha de acesso contra uso indevido. O usuário é responsável por todas as atividades originadas a partir de sua identificação. Acessar somente arquivos e dados pertencentes ao próprio usuário, pertencentes ao domínio público ou devidamente autorizados. Utilizar somente programas legalizados, sendo expressamente proibido o uso de software não licenciado. A utilização da Internet para atividades comerciais seja para compra ou para venda, somente será permitida se o site for considerado seguro e com autorização dos Administradores de Sistema.

6. DAS PROIBIÇÕES

A SOHIDRA considera qualquer violação das normas acima falta grave e passiva de punição nos termos da CLT e estatuto dos servidores públicos do Estado do Ceará, reservando-se o direito de copiar e examinar qualquer arquivo ou informação residente nos sistemas da SOHIDRA, relativo ao uso indevido para identificar e responsabilizar os infratores.

7. PRINCÍPIOS ÉTICOS PARA O USO DE COMPUTADORES NA SOHIDRA

As normas ora estabelecidas delineiam as diretrizes gerais para o uso de recursos computacionais na SOHIDRA. São princípios éticos aplicados diariamente na vida da comunidade que também se aplicam ao uso comunitário de recursos computacionais. Quanto ao uso de tais recursos todos, os servidores da SOHIDRA ou terceirizados têm dois direitos básicos importantes: privacidade e acesso adequado aos recursos computacionais compartilhados. Não é ético que um membro viole os direitos do outro, sob pena e aplicação de penalidades disciplinares.

8. DA PRIVACIDADE

Em sistemas de computação compartilhados, todo usuário possui uma identificação. Ninguém deve usar o sistema utilizando a identificação de outro usuário sem sua permissão explícita. Todos os arquivos têm um responsável, a menos que se tornem disponíveis explicitamente para outros usuários. Todo o tráfego na rede é considerado confidencial. O Administrador de Sistema computacional pode acessar os arquivos de outros usuários somente quando for indispensável para a manutenção do sistema. Se alguma falha na segurança for detectada, esta deverá ser informada ao Administrador do Sistema.

9. CONTIGÊNCIA E CONTINUIDADE

Implantar rotina de backup (cópias), armazenamento, testes de integridade e restore (recuperação) de dados; Definir equipamentos de backup para substituição de ativos com problemas e que são críticos para continuidade do negócio.

Manter os ativos de processamento críticos em áreas seguras e adequadas, protegidos contra perigos ambientais e com implantação de controles de acesso; Proteger os ativos de roubo e modificação, definindo controles de forma a minimizar a perda ou dano; Adotar controles de acesso físico e lógico para uso de ativos no âmbito da SOHIDRA.

Temos Licenças de Antivírus em todas as maquinas e nos Servidores e que nesse é feita periodicamente varreduras constantes para proteção dos nossos Arquivos.

10. DOS RECURSOS

Os recursos computacionais da SOHIDRA devem ser empregados de forma econômica, respeitando o espírito comunitário da instituição. Todos os usuários devem ficar cientes que uma conta de acesso aos sistemas de informação da SOHIDRA, sejam quais forem, podem sofrer auditoria pela Unidade Administrativa de Informática, caso seja necessário dirimir dúvidas sobre o uso indevidos dos recursos.

11. DAS PENALIDADES

As penalidades poderão incluir processos administrativos, criminais e cíveis, além da aplicação das penalidades previstas em lei. Uma vez que o usuário é responsável por qualquer atividade a partir de sua conta, o mesmo responderá por qualquer ação legal apresentada ao Governo do Estado do Ceará que envolva a sua conta de acesso a serviços. No caso de evidências de uso irregular dos recursos de acesso a serviços, o usuário terá seu acesso bloqueado para averiguação. Constatada a irregularidade será realizado o cancelamento do acesso ao serviço e serão aplicadas as penalidades, de acordo com a legislação vigente. O usuário infrator deverá ser notificado e a ocorrência de transgressão comunicada ao seu chefe imediato e à diretoria correspondente. Será designada uma Comissão para avaliação dos possíveis casos de infração, sendo a mesma definida pelo Gestor responsável ou Superintendente da Sohidra.

Superintendência de Obras Hidráulicas – SOHIDRA, em Fortaleza, 29 de Maio de 2023.

Á COMISSÃO DE CONTROLE INTERNO:

LUCIANA LOPES BRANDÃO AMORA
Superintendente Adjunta

FRANCISCO HEMIRTON LEMOS PEIXOTO
Diretor Administrativo-Financeiro

ANA KAREN CARVALHO SARMENTO
Ass. de Desenv. Institucional

DE ACORDO:

PAULO JOSÉ GOMES FERREIRA
Superintendente da SOHIDRA