DECRETO Nº29.226, de 13 de março de 2008.

PRORROGA A VIGÊNCIA E OS EFEITOS DO DECRETO Nº29.162, DE 16 DE JANEIRO DE 2008.

O GOVERNADOR DO ESTADO DO CEARÁ, no uso das atribuições que lhe confere o Art.88 da Constituição do Estado do Ceará, e CONSIDERANDO a relevância do Programa Ronda e das atividades exercidas pelos militares em exercício de policiamento ostensivo do Programa; CONSIDERANDO o disposto nos §2º, parte final, e no §4º do Art.54 da Lei nº13.729, de 11 de janeiro de 2006 (Estatuto dos Militares do Estado do Ceará), acrescidos pelo Art.11 da Lei nº13.768, de 4 de maio de 2006; CONSIDERANDO o disposto no Decreto nº29.162, de 16 de janeiro de 2008, que concede a gratificação prevista no §2º do Art.54, parte final, da Lei nº13.729, de 11 de janeiro de 2006, acrescido pelo Art.11 da Lei nº13.768, de 04 de maio de 2006, aos militares em policiamento ostensivo do Programa Ronda, pelo período que especifica; DECRETA:

Art.1º Ficam prorrogados a vigência e os efeitos do Decreto nº29.162, de 16 de janeiro de 2008, publicado no Diário Oficial do Estado da mesma data, de 01 de março de 2008 até 30 de abril de 2008.

Art.2º Este Decreto entra em vigor na data da sua publicação, com efeitos a partir de 01 de março de 2008.

Art.3º Ficam revogadas as disposições em contrário.

PALÁCIO IRACEMA, DO GOVERNO DO ESTADO DO CEARÁ, em Fortaleza, aos 13 dias do mês de março de 2008.

Cid Ferreira Gomes
GOVERNADOR DO ESTADO DO CEARÁ
Roberto das Chagas Monteiro
SECRETÁRIO DA SEGURANÇA PÚBLICA E DEFESA SOCIAL

*** *** ***

DECRETO Nº29.227, de 13 de março de 2008.

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 COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DO GOVERNO DO ESTADO DO CEARÁ – CGSI.

O GOVERNADOR DO ESTADO DO CEARÁ, no uso das atribuições que lhe confere o art.88, incisos IV e VI, da Constituição Estadual e CONSIDERANDO a necessidade de garantir a integridade, confidencialidade e disponibilidade das informações sob gestão do Governo do Estado do Ceará e definir Diretrizes, Normas e Procedimentos que compõem a Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará a serem implantadas pelos órgãos e entidades estaduais; DECRETA:

Art.1º Este Decreto disciplina a Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará e cria o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI, com sua composição e competências.

Art.2º Fica instituída a Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará, publicada no anexo único deste Decreto;

Parágrafo Único. Os documentos da Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará deverão ficar disponíveis na Internet, no site da Empresa de Tecnologia da Informação do Ceará – ETICE.

Art.3º Fica instituído o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI, vinculado à Secretaria de Planejamento e Gestão – SEPLAG, sob a coordenação da Empresa de Tecnologia da Informação do Estado do Ceará – ETICE, em conformidade com o modelo da Tecnologia da Informação e Comunicação do Governo do Estado do Ceará.

§1º O Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI é um comitê temático de Tecnologia da Informação e Comunicação de caráter técnico, consultivo e permanente, focado em Segurança da Informação, devendo submeter as suas decisões aos órgãos superiores de Tecnologia da Informação e Comunicação do Estado do Ceará.

§2º. O Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI será formado por técnicos representantes dos órgãos e entidades estaduais com conhecimentos em segurança da informação, com indicação de um suplente para cada titular, com a seguinte composição:

I - Um Coordenador, representando a Empresa de Tecnologia da Informação do Estado do Ceará – ETICE;

II - Uma Secretaria Executiva, representada pela Assessoria de Estratégias de Tecnologia da Informação – ASETI da Secretaria de Planejamento e Gestão - SEPLAG;

III - Membros representantes dos seguintes órgãos e entidades estaduais:

Secretária da Secretaria de Planejamento e Gestão – SEPLAG, Casa Civil, Secretaria da Ciência, Tecnologia e Ensino Superior – SECITECE, Secretaria da Fazenda – SEFAZ, Conselho Estadual de Educação – CEC, Gabinete do Governador – GABGOV, Secretaria da Educação – SEDUC, Secretaria da Saúde – SESA, Companhia de Água e Esgoto do Ceará – CAGECE, Departamento Estadual de Trânsito do Ceará – DETRAN, e demais órgãos e entidades convidados pela Secretária da Secretaria de Planejamento e Gestão – SEPLAG.

§3º O representante da Secretária da Secretaria de Planejamento e Gestão – SEPLAG acumulará as funções de Secretaria Executiva e membro do Comitê;

§4º Compete ao Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI:

I - Supervisionar a execução, revisar e atualizar a Política de Segurança da Informação do Governo do Estado do Ceará;

II - Disseminar a cultura e a Política de Segurança da Informação no âmbito do Governo do Estado do Ceará;

III - Analisar e monitorar os incidentes de Segurança da Informação;

IV - Analisar, acompanhar e avaliar as principais iniciativas de Segurança da Informação nos ambientes de TIC dos órgãos e entidades do Governo do Estado do Ceará;

V - Promover a elaboração, atualização, validação e divulgação da Política de Segurança da Informação do Governo do Estado do Ceará;

VI - Promover a elaboração e implantação de planos de contingência e recuperação de desastres;

VII - Coordenar as ações para implantação da Política de Segurança da Informação no âmbito do Governo do Estado do Ceará, e

VIII – Deliberar sobre as questões que lhe tenham sido encaminhadas.

Art.4º A Assessoria de Estratégias de TI - ASETI, juntamente com a Empresa de Tecnologia da Informação do Ceará – ETICE e o Comitê Gestor de Políticas de Segurança dos Ambientes de TIC do Governo do Estado do Ceará - CGSI, serão responsáveis por dirimir eventuais dúvidas e orientar quanto à aplicação da Política instituída no caput do Art.1º deste Decreto.

Art.5º Este Decreto entra em vigor na data de sua publicação.

Art.6º Revogam-se as disposições em contrário.

PALÁCIO IRACEMA, DO GOVERNO DO ESTADO DO CEARÁ, em Fortaleza aos 13 de março de 2008.

Cid Ferreira Gomes
GOVERNADOR DO ESTADO DO CEARÁ
Silvana Maria Parente Neiva Santos
SECRETÁRIA DO PLANEJAMENTO E GESTÃO

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS AMBIENTES DE TIC DO GOVERNO DO ESTADO DO CEARÁ

Política de Segurança dos Ambientes de TIC

Fortaleza, 18 de Setembro de 2007

Sumário

Governador
Cid Ferreira Gomes
Vice-Governador
Francisco José Pinheiro
Secretária do Planejamento e Gestão
Silvana Maria Parente Neiva Santos
Secretária Adjunta do Planejamento e Gestão
Desirée Custódio Mota Gondim
Secretário Executivo do Planejamento e Gestão
Luiz Gonzaga Costa Evangelista

Coordenadora da Assessoria de Estratégias de Tecnologia da Informação (Aseti)
Lícia Viana Bezerra
Articuladores
Ana Lúcia Pereira Gomes
Regina Estela Benevides de Lima
Analista de Gestão de Tecnologia da Informação
Denise Maria Norões Olsen
Analista Auxiliar de Gestão Pública
Nina Rosa Guanabara
Apoio e suporte administrativo
Aurineide Soares de Freitas

Grupo de Trabalho
Denise Maria Norões Olsen – Seplag/Aseti
Regina Estela Benevides de Lima – Seplag/Aseti
Cézar Douglas Pinheiro Fernandes – Seplag
José Alexsandre Fonseca da Silva – Etice
Andréia Oliveira Ferreira – Gabgov
José Clerton Evelmo Farias Júnior – Seduc
Adriana Castelo Branco de P. Vianna – Sesa
Edelson Mendes Vilanova e Silva – Sesa
Otávio Fernandes Costa – Cagece
Vinícius Domingues – Cagece
George Wosley B. N. Lima - Detran

1. Apresentação

A Secretaria de Planejamento e Gestão (SEPLAG), por meio de sua Assessoria de Estratégias de Tecnologia da Informação (ASETI), apresenta a Política de Segurança dos Ambientes de TIC do Governo do Estado do Ceará, no cumprimento do seu papel de órgão central de definição de estratégias de Tecnologia da Informação e Comunicação (TIC), e atendendo à Portaria de Nº317/2007 dessa Secretaria, a qual constituiu um Grupo de Trabalho (GT) para promover estudos e elaborar as Políticas de Segurança para os órgãos e entidades estaduais.

A Política de Segurança da Informação definida neste documento atende à diretriz de Governo de "Rever e aplicar Políticas da Segurança da Informação do Estado", elaborada no Planejamento Estratégico da Função Tecnologia da Informação do Governo do Estado do Ceará, para o período de 2007 a 2016 e é composta de duas seções:

1. Diretrizes que são as regras de alto nível que representam os princípios básicos que o Governo do Estado do Ceará resolveu incorporar a sua gestão e servirão como base para que as normas e os procedimentos sejam criados e detalhados, e
2. Normas que especificam no plano tático os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes e servir como base para os procedimentos no plano operacional.

Posteriormente, a partir da Política traçada neste documento, os órgãos e entidades estaduais deverão desenvolver suas Políticas de Segurança da Informação alinhadas com o Planejamento Estratégico de suas áreas e com foco nas estratégias de Governo definidas com foco na modernização, inclusão digital e governança.

Faz-se, portanto, necessário o acompanhamento permanente da aplicação dessa política pelos órgãos centrais competentes de TIC - ETICE e ASETI, considerando também o caráter dinâmico da segurança da informação no âmbito nacional e internacional.

Ela deve servir como guia para todos os órgãos e entidades estaduais do Poder Executivo Estadual implementarem e manterem a gestão de Segurança da Informação nos seus ambientes de tecnologia da informação e comunicação – TIC.

2. Objetivo

O objetivo desta Política de Segurança é estabelecer diretrizes e normas gerais para a gestão da segurança da informação dos ambientes de TIC do Governo do Estado do Ceará de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, descrevendo procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

3. Abrangência

A Política de Segurança da Informação dos Ambientes de TIC deverá ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes nos Órgãos/ Entidades estaduais, como também às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito do Governo do Estado do Ceará ou a quem quer que venha a ter acesso a dados ou informações, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

4. Responsabilidades

4.1. O Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI tem as seguintes competências:

I. Supervisionar a execução, revisar e atualizar a Política de Segurança da Informação do Governo do Estado do Ceará;
II. Disseminar a cultura e a Política de Segurança da Informação no âmbito do Governo do Estado do Ceará;
III. Analisar e monitorar os incidentes de Segurança da Informação;
IV. Analisar, aprovar, acompanhar e avaliar as principais iniciativas de Segurança da Informação nos ambientes de TIC dos órgãos/ entidades do Governo do Estado do Ceará;
V. Promover a elaboração, atualização, validação e divulgação das Diretrizes, objetivos estratégicos, ações prioritárias, normas e procedimentos da Política de Segurança da Informação do Governo do Estado do Ceará;
VI. Promover a elaboração e implantação de planos de contingência e recuperação de desastres;
VII. Coordenar as ações para implantação das Políticas de Segurança da Informação no âmbito do Governo do Estado do Ceará, e
VIII. Deliberar sobre as questões que lhe tenham sido encaminhadas.

4.2. O responsável pela unidade ou função de gestão de segurança da informação de cada órgão é responsável por:

I. Propor diretrizes, normas e procedimentos de segurança da informação aplicáveis ao seu órgão;
II. Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança em seu órgão;
III. Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação em seu órgão;
IV. Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança em seu órgão, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;
V. Relatar ao dirigente máximo do órgão, para as devidas providências, as ocorrências, eventos e incidentes de segurança da informação, na forma de relatório detalhado e circunstanciado;
VI. Nos órgãos onde não existir unidade de auditoria interna, coordenar e/ou acompanhar a execução de auditorias de segurança nos sistemas de informação no seu órgão.

4.3. Ao gestor de tecnologia da informação de cada órgão cabe a responsabilidade de:

I. Homologar e autorizar o uso de sistemas e dispositivos de processamento de informações em suas instalações,
II. Suspender, a qualquer tempo, o acesso do usuário a recurso computacional da Previdência Social quando evidenciados riscos à segurança da informação e informar o incidente ao gestor de segurança da informação do órgão.
III. Nos órgãos onde não existir o responsável pela unidade ou função de gestão de segurança da informação, assumir as responsabilidades a ele definidas no item 4.3.

4.4. A Chefia Imediata de cada órgão cabe a responsabilidade de:

I. Disseminar permanentemente a Política de Segurança da Informação;
II. Garantir o cumprimento da Política de Segurança da Informação;
III. Solicitar a disponibilidade ou cancelamento dos recursos de informática necessários aos seus subordinados para o bom desempenho de suas funções

4.5. Ao Usuário de cada órgão cabe a responsabilidade de:

I. Conhecer e seguir a Política de Segurança da Informação;
II. Notificar a sua chefia imediata ou a qualquer membro do Comitê Gestor de Segurança da Informação indício ou falha na Segurança da Informação.
III. Responder por toda atividade executada por meio de sua identificação.

5. Seções

5.1. Diretrizes Gerais do Governo do Estado do Ceará para Segurança da Informação

Diretriz 1:

Uma Política de Segurança da Informação deve ser implementada de forma a orientar estrategicamente as ações de segurança a serem executadas pelos órgãos/entidades do Governo do Estado do Ceará.

Objetivo Estratégico	Ações Prioritárias
Desenvolver e implantar uma Política de Segurança da Informação nos órgãos/entidades do Governo do Estado do Ceará.	1. Adotar mecanismos para promover a elaboração, revisão, atualização, divulgação, conscientização e validação das diretrizes, normas e procedimentos da Política de Segurança da Informação nos órgãos/entidades estaduais; 2. Elaborar plano estratégico de segurança da informação para viabilizar todos os recursos necessários para o cumprimento das Políticas; 3. Selecionar mecanismos de segurança da informação considerando fatores de riscos, tecnologias e custos; 4. Criar nos órgãos/entidades estaduais grupo responsável pela elaboração, implantação, acompanhamento, auditoria e revisão da Política de Segurança da Informação; 5. Criar comitê de gestão de segurança da informação para coordenar a política de segurança do Governo do Estado do Ceará, e 6. Estabelecer mecanismos que possibilitem o processo de coleta, recuperação, análise e correlacionamento de dados para investigação de questões cíveis, criminais e administrativas, para proteger os usuários e recursos de TIC.
Comunicar oficialmente e capacitar todos os usuários na Política de segurança adotada pelo Governo do Estado do Ceará, para garantir a conscientização e a prática.	1. Definir mecanismos para garantir a disseminação da cultura de segurança da informação nos órgãos/entidades estaduais; 2. Estabelecer junto aos órgãos/entidades estaduais medidas para que a política de segurança seja cumprida de forma que as diretrizes, normas e procedimentos de segurança sejam aplicados por todos os usuários, e 3. Prover mecanismos de capacitação nos procedimentos de segurança e uso correto dos recursos de TI para todos os usuários.

Diretriz 2:

Toda informação dos órgãos/entidades do Governo do Estado do Ceará deve ter uma classificação que defina seu grau de confidencialidade, disponibilidade e criticidade, bem como uma política para acesso e manuseio das mesmas.

Objetivo Estratégico	Ações Prioritárias
Implantar uma metodologia de classificação de informações e conhecimentos no âmbito do Governo do Estado do Ceará.	1. Desenvolver processo de classificação da informação para definir níveis e critérios adequados, e 2. Estabelecer normas, padrões e procedimentos relacionados a produção, tramitação, transporte, manuseio, custódia, armazenamento, conservação e eliminação de documentos no âmbito do Governo do Estado do Ceará.
Garantir de forma segura o acesso e manuseio das informações no âmbito do Governo do Estado do Ceará	1. Definir normas e procedimentos de acesso a dados, informações e conhecimentos por pessoas do próprio órgão/entidade, por outros órgãos/entidades e terceiros.

Diretriz 3:

Normas e responsabilidades pela gestão dos ativos de TI, devem ser estabelecidas de forma a garantir a continuidade do negócio do Governo do Estado do Ceará.

Objetivo Estratégico	Ações Prioritárias
Definir procedimentos de rotina para a execução de cópias de segurança e disponibilização dos recursos de reserva.	1. Implantar rotina de backup (cópias), armazenamento testes de integridade e restore (recuperação) de dados; 2. Definir equipamentos de backup para substituição de ativos com problemas e que são críticos, e 3. Implantar normas e responsabilidades sobre o controle das mídias de software.
Adotar critérios relacionados ao uso de ativos de processamento no Governo do Estado do Ceará.	1. Manter os ativos de processamento críticos em áreas seguras e adequadas, protegidos contra perigos ambientais e com implantação de controles de acesso; 2. Inventariar os ativos, classificando-os quanto a importância, prioridade e nível de proteção; 3. Proteger os ativos de roubo e modificação, definindo controles de forma a minimizar a perda ou dano; 4. Adotar controles de acesso físico e lógico para uso de ativos no âmbito do Governo do Estado do Ceará; 5. Estabelecer processos de aquisição de bens e serviços baseados em preceitos legais; 6. Aprimorar e/ou definir critérios de seleção, movimentação ou desligamento de pessoal que impactam na segurança da informação, e 7. Implementar mecanismos de registro de históricos dos ativos de TI, garantindo a sua rastreabilidade.

Objetivo Estratégico	Ações Prioritárias
Desenvolver e implementar plano de contingência e respostas a incidentes de forma a assegurar a continuidade do negócio, bem como o seu reestabelecimento em situação de anormalidade.	1. Definir os processos e recursos críticos realizando analise e impacto de riscos para elaboração do plano de continuidade do negócio; 2. Estabelecer processos de proteção contra falhas e danos que comprometam as atribuições do Governo do Estado do Ceará; 3. Definir mecanismos formais e periodicamente testados para garantir a continuidade das atividades críticas e o retorno à situação de normalidade, e 4. Definir processo e criar procedimentos para gestão de incidentes.

Diretriz 4:
Normas relativas ao desenvolvimento, aquisição e implantação de sistemas computacionais devem garantir a interoperabilidade e a obtenção de níveis de segurança adequados.

Objetivo Estratégico	Ações Prioritárias
Assegurar que os sistemas de processamento em operação e em implantação possuam documentação suficiente para garantir sua manutenibilidade, instalação e utilização.	1. Definir e implantar metodologias de desenvolvimento de sistemas implementando requisitos de segurança. 2. Implantar a cultura de documentação de sistemas de processamento como manuais técnicos e operacionais, e 3. Definir procedimentos para controle de liberação de softwares.
Garantir que apenas pessoas autorizadas tenham acesso a funcionalidades e informações dos sistemas de processamento.	1. Manter controle de acesso a todos os sistemas utilizando identificação de uso pessoal e intransferível e com validade estabelecida, que permita de maneira clara o seu reconhecimento; 2. Prever trilhas de auditoria nos sistemas de processamento críticos, e 3. Definir controles para que usuários detenham acesso apenas aos recursos necessários e imprescindíveis ao desenvolvimento do seu trabalho.
Estabelecer que as condições e termos de licenciamento de softwares e direitos de propriedade intelectual devam ser respeitados.	1. Definir normas para instalação de softwares com objetivo de combater a pirataria; 2. Garantir o controle das licenças de softwares utilizados pelo órgão/entidade do Governo do Estado do Ceara; 3. Adotar procedimentos para que a instalação e uso de softwares e sistemas computacionais, devam ser homologados e autorizados pelo setor competente do órgão/entidade, e 4. Definir mecanismos para cessão de softwares e sistemas computacionais no âmbito do Governo do Estado do Ceará.

Diretriz 5:
Os órgãos e entidades devem estabelecer e gerenciar um conjunto de regras que possibilitem a utilização adequada da Internet e correio eletrônico.

Objetivo Estratégico	Ações Prioritárias
Estabelecer responsabilidades e requisitos básicos de utilização da Internet e correio eletrônico no âmbito do Governo do Estado do Ceará.	1. Elaborar plano de comunicação para conscientização de que o uso da internet e correio eletrônico não é um direito e sim uma concessão; 2. Disseminar o conceito de não privacidade do uso da Internet e correio eletrônico.
Assegurar que todos os usuários ao utilizarem esses serviços deverão fazê-los no estrito interesse dos órgãos e entidades mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.	1. Implantar mecanismos de autenticação e monitoramento, que determinem a titularidade de todos os acessos à Internet e correio eletrônico, e 2. Criar mecanismos de controle da demanda e da disponibilidade, garantindo a qualidade do serviço.

5.2. Normas

Identificação	Título da Norma	Objetivo
NPS01	Uso do Correio eletrônico	Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico no âmbito do Governo do Estado do Ceará.
NPS02	Uso da Internet	Estabelecer responsabilidades e requisitos básicos de uso dos serviços de acesso a Internet no âmbito do Governo do Estado do Ceará.
NPS03	Contas e Senhas para Usuários	Estabelecer os procedimentos adequados para a correta utilização das contas de usuários no ambiente de Tecnologia da Informação e Comunicação – TIC no âmbito do Governo do Estado do Ceará.
NPS04	Contas e Senhas para Administradores	Estabelecer os procedimentos adequados para a correta utilização das contas com privilégios de Administrador de sistemas e serviços no âmbito do Governo do Estado do Ceará.
NPS05	Gestão Ativos	Estabelecer os procedimentos adequados para alcançar e manter a proteção adequada dos ativos do ambiente de Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Ceará, de forma a resguardar empregados, colaboradores e o Governo do Estado do Ceará contra ações ilegais e que gerem perda de dados e/ou prejuízos à imagem do Governo.
NPS06	Contingência e Continuidade do Negócio	Estabelecer os procedimentos adequados para montagem do plano de contingência adequado para os elementos que impactam diretamente no ambiente de Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Ceará, de forma dar continuidade dos negócios, quando houver algum tipo de interrupção nos ativos críticos do Governo.

6. Penalidades

O não cumprimento das determinações desta Política de Segurança sujeita o infrator às penalidades previstas em lei e regulamentos internos dos órgãos.

USO DO CORREIO ELETRÔNICO

NORMA NPS01

USO DO CORREIO ELETRÔNICO (e-mail)

1. Apresentação

Prover a comunicação é, sem dúvida, a essência das redes. As pessoas sempre procuraram se corresponder da maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é a aplicação que mais ilustra esta procura, pois reúne, entre outros, estes atributos. Entretanto, a facilidade de correio eletrônico fornecido pelo Governo do Estado do Ceará, deve ser usada no interesse do serviço, podendo ser, ocasionalmente, utilizada para mensagens pessoais curtas e pouco freqüentes.

Considerando que o uso dos serviços de Correio Eletrônico, 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 desse importante recurso tecnológico.

Todos os Usuários ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do Órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público.

2. Objetivo

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico no âmbito do Governo do Estado do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará.

4. Definições

Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004]

Caixa Postal/Correio eletrônico – Espaço em disco, onde são armazenadas as mensagens de correio eletrônico.

Correio Eletrônico – Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.

Criptografia – Ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

FTP (File Transfer Protocol) – Protocolo padrão da Internet, usado para transferência de arquivos entre computadores.

IMAP (Internet Message Access Protocol) – Protocolo de acesso a mensagens eletrônicas.

Internet – Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

Intranet – Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os funcionários possam acessar as informações dos seus respectivos Órgãos Públicos.

Órgão Público – Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

POP (Post Office Protocol). – Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

Servidor de Correio Eletrônico – Equipamento que provê o serviço de envio e recebimento de mensagens de correio eletrônico.

SMTP (Simple Mail Transfer Protocol) – Protocolo de comunicação usado para troca de mensagens na Internet, via correio eletrônico.

Spam – Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado.

Usuários – funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

Vírus Eletrônico – São pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.

5. Abrangência

Esta norma deverá ser aplicada aos ativos de informação e comunicação do Governo do Estado do Ceará.

6. 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 do Governo do Estado do Ceará.

7. Procedimentos

7.1. Criação/Exclusão de conta de e-mail

Para Obter uma conta de e-mail:

- A chefia imediata deverá solicitar ao setor de TIC, por meio de memorando ou e- mail, informando: nome completo do usuário, setor no qual está desempenhando suas atividades, matrícula e justificativa da necessidade da conta de e-mail.
- O setor de TIC efetuará o cadastro e informará ao interessado: o seu usuário, senha padrão/provisória e Normas de uso do e-mail.
- O gestor imediato será responsável pelas contas de e-mail pertencentes ao seu setor.

Para Excluir uma conta de e-mail:

- O gestor imediato deverá solicitar ao setor de TIC, através de memorando ou e-mail, informando: nome completo do usuário, setor no qual está desempenhando suas atividades e matrícula.
- Quando da mudança de setor ou desligamento, o gestor imediato deverá comunicar
  ao setor de TIC para que o remanejamento do usuário seja realizado.
- Os usuários que estiverem utilizando conta de e-mail de forma inadequada
  (conforme política de e-mail) terá sua conta inicialmente bloqueada e será comunicado ao seu gestor imediato para adoção das medidas cabíveis.

8. Regras Gerais

- Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização;
- Os usuários poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet, a critério do titular de Área/Gerência, enquanto perdurar o seu vínculo com a Autarquia;
- Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens;
- O tamanho das caixas postais será de 80 Mbytes para os usuários classificados como VIP´S (Secretários, Presidentes, Diretores e Assessores) e de 40 Mbytes para os demais usuários;
- As mensagens com arquivos anexados (texto e anexo) serão transmitidas conforme os critérios abaixo:

TAMANHO	HORÁRIO	OBS
Até 4 MB	De 06:00 às 00:00 horas	
De 4,1 a 8,0 MB	De 00:01 às 05:59 horas	
Acima de 8,0 MB		Utilizar outro meio de transmissão (p.ex: FTP)

9. Deveres, Responsabilidades e Recomendações

9.1. Deveres do Usuário

- Não enviar mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade do Governo;
- Não utilizar o e-mail do órgão para assuntos pessoais;
- Adotar o hábito de leitura dos e-mails diariamente;
- Enviar e-mails apenas para destinatários que realmente precisam da informação.
- Não acessar, quando não autorizado, a caixa postal de outro usuário e ao Banco de Dados do Correio Eletrônico de outro Órgão;
- Não enviar, armazenar e manusear material que contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública;
- Não enviar, armazenar e manusear material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
- Não enviar, armazenar e manusear material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação

ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;

- Não deve utilizar o sistema de correio para envio de mensagens do tipo "corrente", aviso de vírus, criança desaparecida, criança doente, pague menos em alguma coisa, etc.;
- Não utilizar as listas e/ou caderno de endereços do Governo ou de qualquer Órgão para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
- Não usar contas particulares, através dos serviços Post Office Protocol - POP, Internet Message Access Protocol - IMAP e Simple Mail Transfer Protocol - SMTP de provedores não pertinentes ao domínio ce.gov.br;
- Deve evitar todo e qualquer procedimento de uso do Correio Eletrônico não previsto nesta Política, que possa afetar de forma negativa o Órgão ou o Governo.

9.2. Responsabilidades do Usuário

- O usuário é o responsável pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;
- O mau uso de uma conta de correio por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;
- É de exclusiva responsabilidade do usuário o conteúdo de seus arquivos;

9.3. Responsabilidades do Administrador do Correio

- Verificar periodicamente a conta postmaster, para detectar eventuais problemas que possam estar ocorrendo no servidor e na entrega de e-mail dos usuários;
- Criação das contas "security" e "abuse" nos servidores de domínio;
- Implementar o papel de moderador nas listas, como objetivo de evitar spans.

9.4. Recomendações para o Administrador do Correio

- Configurar o servidor de correio para enviar e-mail só após a autenticação do Usuário, utilizando configurações do tipo "smtp auth", "smtp after pop", etc.
- Implementar medidas para filtragem de vírus no sistema de correio eletrônico.
- Implementar medidas para filtragem de spam e e-mails indesejados (correntes, mensagens pornográficas, propaganda, etc.) no sistema de correio eletrônico.
- Monitorar o funcionamento do servidor de correio eletrônico, em termos de número de conexões, número de mensagens enviadas e recebidas, número de mensagens bloqueadas, banda consumida na rede, etc.

10. Penalidades

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 e que envolva a sua conta.

No caso de evidências de uso irregular dos recursos de Correio Eletrônico, o usuário terá seu acesso bloqueado para averiguação. Constatada a irregularidade será realizado o cancelamento da caixa do correio eletrônico 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.

NORMA NPS02

USO DA INTERNET

1. Apresentação

A Internet é uma grande rede de computadores espalhados por todo o mundo e que podem trocar informações entre si. Entretanto, a facilidade de acesso a Internet fornecido pelo Governo do Estado do Ceará, deve ser usada no interesse do serviço.

Considerando que o uso dos serviços de acesso a Internet, 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 desse importante recurso tecnológico.

Todos os Usuários ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do Órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público.

2. Objetivo

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de acesso à Internet no âmbito do Governo do Estado do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará.

4. Definições

Ativo – qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004]

Modem – Equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações.

Criptografia – Ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

FTP (File Transfer Protocol) – Protocolo padrão da Internet, usado para transferência de arquivos entre computadores.

IMAP (Internet Message Access Protocol) – Protocolo de acesso a mensagens eletrônicas.

Internet – Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

Intranet – Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os funcionários possam acessar as informações dos seus respectivos Órgãos Públicos.

Órgão Público – Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

Site – Páginas contendo informações, imagens, fotos, vídeos, sons, etc., que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte a rede.

Software – Programa de Computador.

Download – Baixar um arquivo ou documento de outro computador, através da Internet.

Upload – Envio de um arquivo de seu computador para outro, através da Internet.

Peer-to-Peer (P2P) – É um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet.

URL - Universal Resource Locator - LINK ou endereço de uma página Web, como por exemplo http://www.seplag.ce.gov.br/.

Usuários – funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

Códigos Maliciosos ou Agressivos – Qualquer código adicionado, modificado ou removido de um Sistema, com a intenção de causar dano ou modificar o funcionamento correto desse Sistema, como por exemplo, vírus eletrônico.

Vírus Eletrônico – São pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.

5. Abrangência

Esta norma deverá ser aplicada a todos os usuários que possuam acesso à Internet provida do Governo do Estado do Ceará.

6. 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 do Governo do Estado do Ceará.

7. Procedimentos

7.1. Criação/Exclusão de conta de acesso à Internet

Para Obter uma conta:

- A chefia imediata deverá solicitar ao setor de TIC, por meio de memorando assinado, informando: nome completo do usuário, setor no qual está desempenhando suas atividades, matrícula e justificativa da necessidade da conta de acesso à Internet.
- O setor de TIC efetuará o cadastro e informará ao interessado: o seu usuário, senha padrão/provisória e Normas de uso da Internet;
- A senha deve ser confidencial e não compartilhada.
- O gestor imediato será responsável pelas contas de acesso à Internet pertencentes ao seu setor.

Para Excluir uma conta:

- O gestor imediato deverá solicitar ao setor de TIC, por

meio de memorando assinado, informando: nome completo do usuário, setor no qual está desempenhando suas atividades e matrícula.
- Quando da mudança de setor ou desligamento, o gestor imediato deverá comunicar ao setor de TIC para que o remanejamento do usuário seja realizado.

8. Regras Gerais
- O acesso à Internet, no âmbito do Governo do Estado do Ceará, é uma concessão e não um direito. Portanto a sua utilização deve ser para atividades inerentes aos trabalhos desenvolvidos.
- O acesso à Internet é feito unicamente pela conexão provida pelo órgão, ficando proibida a utilização diferente desta.
- Todas as contas de acesso à Internet terão uma titularidade, determinando a responsabilidade sobre a sua utilização;
- O acesso à Internet será monitorado por meio de ferramentas próprias, podendo os acessos serem auditados quando necessário. Todos os registros de acessos à Internet são passíveis de auditoria;
- É expressamente proibido o acesso à Internet para violar leis e regras brasileiras ou de qualquer outro país. O uso dos recursos de Internet provido pelo Governo do Estado do Ceará para atividades ilegais é razão para perda de privilégios e ações administrativas cabíveis;
- Somente usuários autorizados a falar, analisar ou publicar documentos em nome do
  Governo do Estado do Ceará poderão fazê-los em comunicações eletrônicas;
- O Governo do Estado do Ceará mantém o direito de cópia de todo material postado na Internet por qualquer usuário no curso de suas obrigações;
- São consideradas como práticas não aceitáveis para acesso à Internet:
  - Material de propaganda política, racismo, terrorismo, hacker, assédio sexual, pornografia, pedofilia, incentivo a violência, descriminação e outros não condizentes com os objetivos de trabalho do Governo do Estado do Ceará;
  - Sites de conversação (bate-papo);
  - Sites de relacionamentos como Orkut, Gazzag e afins;
  - Sites de Proxy;
  - Sites de qualquer tipo de jogos, inclusive jogar pela Internet;
  - Programas que implementem P2P, onde o computador do usuário atua como servidor, como Kazaa, Emule, Net-Meeting, Napster, Groove, ICQ, Morpheus e afins.
  - Web rádio e Web TV (sessões de transmissão contínua de vídeo e áudio)
  - Baixar arquivos (downloads) de som (mp3) e vídeo ou executar arquivos do tipo exe, dat, sys, bat e outros tipos de arquivos executáveis.
  - Distribuir software ou conteúdo não autorizado (pirataria);
  - Disseminar vírus, vermes, cavalos de tróia ou qualquer outro tipo de código malicioso;
  - Fazer download de programas não relacionados as atividades fins e acessórias do Governo do Estado do Ceará;
  - Adotar de forma independente do setor de TIC, quaisquer mecanismos de codificação/criptografia;
- Os usuários da Internet somente deverão realizar downloads de grandes arquivos (acima de 4Mb) fora do horário de expediente, para não comprometer o funcionamento da infra-estrutura de computação do Governo do Estado do Ceará;
- Serão bloqueados sites de pornografia, pedofilia e outros contrários a Lei e as definições desta Norma;
- Se algum usuário souber sobre qualquer violação a esta Norma deverá comunicar ao Setor competente de TIC ou a sua chefia imediata.

9. Deveres, Responsabilidades e Recomendações

9.1. Deveres do Usuário
- Utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos, a ordem pública e as definições desta Norma;
- Evitar utilizar a Internet, para a prática de atos ilícitos, proibidos pela lei ou pela presente Norma, como também danificar e/ou sobrecarregar os recursos tecnológicos (hardware e software);
- Quando preencher um formulário ou enviar informações confidenciais por meio da Internet deve certificar-se que a conexão está segura através do símbolo do cadeado fechado (SSL) que aparece no canto inferior direito do browser e da palavra HTTPS substituindo a palavra HTTP na barra de endereço do browser, para certificar que os dados estão sendo enviados de forma segura pela Internet;
- Desconectar-se imediatamente de um site que contenha acesso restrito, mesmo que tenha sido aceito pelos sistemas encarregados de barrá-lo;
- Evitar advogar causas políticas e de emitir informações não autorizadas sobre quaisquer serviços, produtos, contextos políticos, dentre outros na Internet.

9.2. Responsabilidades do Usuário
- O usuário é o responsável pelos acessos à Internet realizados pela sua conta;
- O mau uso de uma conta de acesso à Internet por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;
- Zelar pelo fiel cumprimento ao estabelecido nesta Norma;

9.3. Responsabilidades do Administrador da Internet
- Implantar apenas um ponto de conexão à Internet, para que todos os usuários se autentiquem neste ponto;
- Implantar mecanismos de monitoramento dos acessos à Internet;
- Arquivar todas as solicitações de acesso à Internet para controle;
- Adotar mecanismos de criptografia/codificação para transferência de informações sensíveis pela Internet;
- Verificar periodicamente os acessos à Internet, para detectar eventuais problemas que possam estar ocorrendo;
- Fornecer, quando solicitado pela direção, relatório de acessos dos usuários;
- Definir e homologar browser (navegador) a ser utilizado e prover mecanismos de atualizações e correções de segurança;
- Bloquear sites que vão de encontro a esta Norma e que estejam comprometendo o bom funcionamento dos recursos de Internet;

10. 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 à Internet.

No caso de evidências de uso irregular dos recursos de acesso à Internet, o usuário terá seu acesso bloqueado para averiguação. Constatada a irregularidade será realizado o cancelamento do acesso à Internet 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.

NORMA NPS03

CONTAS E SENHAS PARA USUÁRIOS

1. Apresentação

Considerando que o uso inapropriado de senhas, possa vir a comprometer o funcionamento da infra-estrutura de segurança da informação do Governo do Estado do Ceará, é de suma importância que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços.

2. Objetivo

Estabelecer os procedimentos adequados para a correta utilização das contas de usuários no ambiente de Tecnologia da Informação e Comunicação –TIC no âmbito do Governo do Estado do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará.

4. Definições

Ativo – qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004]

Código de Acesso – Código de acesso atribuído a cada Usuário. A cada código de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos computacionais disponíveis.

Administrador – contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas;

Órgão Público – qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

Usuários – funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

5. Abrangência

Esta norma abrange todos os usuários que possuem ou são responsáveis por uma conta ou qualquer forma de acesso que necessite de senha no ambiente de Tecnologia da Informação e Comunicação – TIC do Governo do Estado do Ceará.

6. 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 do Governo do Estado do Ceará.

7. Procedimentos

7.1. Criação/Exclusão de conta de acesso a serviços

Para Obter uma conta:

- A chefia imediata deverá solicitar ao setor de TIC, por meio de memorando assinado, informando: nome completo do usuário, setor no qual está desempenhando suas atividades, matrícula e justificativa da necessidade da conta de acesso a qual serviço: Rede, Internet, Correio Eletrônico, Sistemas e Dados;
- O setor de TIC efetuará o cadastro e informará ao interessado: o seu usuário, senha provisória e Política de Segurança, por e-mail ou telefone;
- A senha deve ser confidencial não compartilhada e trocada pelo usuário no primeiro acesso;
- O gestor imediato será responsável pelas contas de acesso pertencentes ao seu setor.

Para Excluir uma conta ou acesso a um serviço:

- O gestor imediato deverá solicitar ao setor de TIC, por meio de memorando assinado, informando: nome completo do usuário, acesso que deve ser removido e justificativa da exclusão;
- Quando da mudança de setor ou desligamento, o gestor imediato deverá comunicar ao setor de TIC para que o remanejamento do usuário seja realizado.

8. Regras Gerais

- Toda conta de usuário precisa possuir senha e deve seguir os padrões estabelecidos nesta Norma;
- Todas as senhas de usuários de acesso a rede, sistemas e serviços diversos do Governo do Estado do Ceará deverão ser trocadas de 3 em 3 meses.
- As contas de rede serão bloqueadas depois de 5 (cinco) tentativas inválidas de entrada. Para destravar o usuário deverá entrar em contato com o setor de TIC;
- Na criação de uma nova conta, o usuário receberá uma senha temporária, a qual deverá ser trocada no primeiro acesso;
- As contas que ficarem inativas por mais de 90 (noventa) dias corridos serão bloqueadas;
- A senha deverá conter no mínimo 6 (seis) caracteres;
- Não utilizar para criação de senhas:
  - O mesmo nome do usuário para senha. Ex: usuário: maria, senha: maria;
  - Seu nome ou combinações deste;
  - Nomes de familiares, datas de aniversário, número de telefone;
  - Informações pessoais ou fáceis de serem obtidas;
  - Uma senha com os mesmos números e letras. Ex: 111111, aaabbb;
  - Palavras que existam em dicionários, catálogos ou listas conhecidas, mesmo que escrita de trás para frente;
  - Utilizar para criação de senhas:
  - Senhas alfa-numéricas. Ex: Ip25O4;
  - Senhas mistas com caixa alta e baixa. Ex: IpSTma
  - Caracteres especiais tipo #, @, $,%, &, !, *, ?, _,/, <>,:,;, {}, [], =, +
  - Se algum usuário souber sobre qualquer violação a esta Norma deverá comunicar ao Setor competente de TIC ou a sua chefia imediata.

9. Deveres, Responsabilidades e Recomendações

9.1 Deveres do Usuário

- Trocar a senha temporária no primeiro acesso;
- Não registrar a senha em papel, em local visível, no computador ou na Internet;
- Nunca utilizar o recurso de "Relembrar a senha" ou semelhantes de aplicações como navegadores, correio eletrônico, entre outras;
- Trocar a senha quando houver suspeita de haver sido comprometida e comunicar o incidente ao setor de TIC;
- Não revelar senhas pelo telefone, e-mail ou por qualquer outro meio para NINGUÉM, mesmo que seja o chefe, assistentes ou secretárias;
- Não revelar senhas em questionários ou formulários;
- Não permitir que alguém observe você digitando sua senha;
- Não revelar senhas para colegas de trabalho enquanto estiver de férias ou licença;

9.2. Responsabilidades do Usuário

- O usuário é o responsável pelos acessos aos serviços realizados pela sua conta;
- O mau uso de uma conta de acesso aos serviços por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;
- Zelar pelo fiel cumprimento ao estabelecido nesta Norma;

9.3. Responsabilidades do Setor de TIC

- Criar e manter as contas de sistemas e serviços;
- Adotar mecanismos para bloquear a senha após 5 (cinco) tentativas inválidas;
- Adotar mecanismos para não aceitar senha com menos de 6 (seis) caracteres;
- Adotar mecanismos para forçar o usuário a trocar a senha no primeiro acesso;
- Instruir os usuários na criação de senhas e a sua importância na segurança da informação.
- Adotar mecanismos de periodicamente enviar para as chefias imediatas, uma relação das contas em quais serviços que estão sob sua responsabilidade.

10. 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.

NORMA NPS04

CONTAS E SENHAS PARA ADMINISTRADORES

1. Apresentação

Considerando que o uso inapropriado de privilégios de administrador de sistemas e serviços, possa vir a comprometer o funcionamento da infra-estrutura de segurança da informação do Governo do Estado do Ceará é de suma importância que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços.

2. Objetivo

Estabelecer os procedimentos adequados para a correta utilização das contas com privilégios de Administrador de sistemas e serviços no âmbito do Governo do Estado do Ceará.

3. Documentos de referência

Diretrizes da Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará.

4. Definições

Ativo - qualquer coisa que tenha valor para a organização [ISO/ IEC 13335-1:2004]

Código de Acesso – Código de acesso atribuído a cada Usuário. A cada código de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos computacionais disponíveis.

Administrador – contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas;

Proprietário do ativo – Identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo. [ISO/IEC 13335-1:2004 Item 7.1.2]

Custodiante do ativo – Identifica uma pessoa ou organismo que cuida do ativo no dia-a-dia [ISO/IEC 13335-1:2004 Item 7.1.2];

Órgão Público – Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

Usuários – funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

5. Abrangência

Esta norma abrange todos os usuários que possuem ou são responsáveis por uma conta ou qualquer forma de acesso com privilégios de "administrador" no ambiente de Tecnologia da Informação e Comunicação - TIC do Governo do Estado do Ceará.

6. 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 do Governo do Estado do Ceará.

7. Procedimentos

7.1. Criação/Exclusão de conta de acesso a serviços

Para Obter uma conta:

- A chefia imediata deverá solicitar ao setor de TIC, por meio de memorando assinado, informando: nome completo do usuário, setor no qual está desempenhando suas atividades, matrícula e justificativa da necessidade da conta de acesso a qual serviço: Rede, Internet, Correio Eletrônico, Sistemas e Dados;
- O setor de TIC efetuará o cadastro e informará ao interessado: o seu usuário, senha provisória e Política de Segurança, por e-mail ou telefone;
- A senha deve ser confidencial não compartilhada e trocada pelo usuário no primeiro acesso;
- O gestor imediato será responsável pelas contas de acesso pertencentes ao seu setor.

Para Excluir uma conta ou acesso a um serviço:

- O gestor imediato deverá solicitar ao setor de TIC, por meio de memorando assinado, informando: nome completo do usuário, acesso que deve ser removido e justificativa da exclusão;
- Quando da mudança de setor ou desligamento, o gestor imediato deverá comunicar ao setor de TIC para que o remanejamento do usuário seja realizado.

8. Regras Gerais

- Toda conta com privilégio de administrador precisa possuir senha e deve seguir os padrões estabelecidos nesta Norma;
- A senha deverá conter no mínimo 10 (dez) caracteres. No caso dos ambientes que não suportarem o mínimo de 10 caracteres, deverão ser utilizados o limite máximo que o ambiente permitir;
- Os sistemas e aplicações deverão prover algum mecanismo ou instrução que garanta que só sejam aceitas senhas com a formação de mínimo de 10 caracteres ou conforme o ambiente;
- As contas com privilégio de administrador não poderão conter em sua formação algo que as identifique como sendo uma conta de administrador. (Ex: Admin, Adm, Administrador, Administrator, pradmin etc.);
- Deverá ser criada uma ou mais contas, sem nenhum privilégio, com formação que possa identificá-la como sendo uma conta de administrador. Essas contas deverão ser constantemente submetidas à auditoria, com o propósito de se verificar as tentativas de utilização das mesmas;
- Não utilizar para criação de senhas:
  - O mesmo nome do usuário para senha. Ex: usuário: maria, senha: maria;
  - Seu nome ou combinações deste;
  - Nomes de familiares, datas de aniversário, número de telefone;
  - Informações pessoais ou fáceis de serem obtidas;
  - Uma senha com os mesmos números e letras. Ex: 111111, aaabbb;
  - Palavras que existam em dicionários, catálogos ou listas conhecidas, mesmo que escrita de trás para frente;
- Utilizar para criação de senhas:
  - Senhas alfa-numéricas;
  - Senhas mistas com caixa alta e baixa;
  - Caracteres especiais tipo #, @, $,%, &, !, *, ?, _,/, <>,:,;, {}, [], =, +
- Deverá ser guardado um histórico composto de, pelo menos, das 8 (oito) últimas senhas;
- A conta deverá ser bloqueada após a 5ª (quinta) tentativa inválida de entrada;
- O tempo de vida das senhas deverá obedecer aos seguintes critérios:
- Administrador de Servidores e de Domínio – validade de 90 (noventa) dias, devendo ser forçada a troca no primeiro login após esse período;
- Administrador Local – Válida por tempo indeterminado.
- O mau uso de uma conta de acesso aos serviços por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;
- No caso de suspeita do comprometimento de uma senha, esta deverá ser reinicializada.
- Se algum usuário souber sobre qualquer violação a esta Norma deverá comunicar ao Setor competente de TIC ou a sua chefia imediata.

9. Recomendações

- Não registrar a senha em papel, em local visível, no computador ou na Internet;
- Nunca utilizar o recurso de "Relembrar a senha" ou semelhantes de aplicações como navegadores, correio eletrônico, entre outras;
- Não revelar senhas pelo telefone, e-mail ou por qualquer outro meio para NINGUÉM;
- Não revelar senhas em questionários ou formulários;
- Não permitir que alguém observe você digitando sua senha;
- Não revelar senhas para colegas de trabalho enquanto estiver de férias ou licença;
- Zelar pelo fiel cumprimento ao estabelecido nesta Norma;

10. 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.

O usuário infrator deverá ser notificado e a ocorrência de transgressão comunicada ao seu chefe imediato e à diretoria correspondente.

NORMA NPS05

GESTÃO DE ATIVOS

1. Apresentação

Considerando a necessidade de alcançar e manter a proteção adequada dos ativos de tecnologia da informação (informação, software, equipamentos, serviços de iluminação, refrigeração, pessoas, reputação e imagem) o Governo do Estado do Ceará considera de grande a implementação de procedimentos formais, de forma a definir claramente quais as responsabilidades que os gestores do Governo do Estado do Ceará terão ao serem designados como proprietário e/ou custodiante de algum ativo.

2. Objetivo

Estabelecer os procedimentos adequados para alcançar e manter a proteção adequada dos ativos do ambiente de Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Ceará, de forma a resguardar empregados, colaboradores e o Governo do Estado do Ceará contra ações ilegais e que gerem perda de dados e/ou prejuízos à imagem do Governo.

3. Documentos de referência

Diretrizes da Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará.

4. Definições

Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004]

Ativos de Informação – Bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisas, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas.[ISO/IEC 13335-1:2004];

- Ativos de Software – Aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.
- Ativos Físicos – Equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos.
- Ativos Serviços – Serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração.
- Ativos Pessoas – Pessoas e suas qualificações, habilidades e experiências.

- Ativos Intangíveis – reputação e imagem da organização.

Proprietário – Identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. Não significa que a pessoal realmente tenha qualquer direito de propriedade ao ativo [ISO/IEC 13335-1:2004].

Custodiante do ativo – Identifica uma pessoa ou organismo que cuida do ativo no dia-a- dia [ISO/IEC 13335- 1:2004].

Confidencialidade – A informação somente pode ser acessada por pessoas explicitamente autorizadas; É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

Disponibilidade – A informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária;

Integridade – A informação deve ser retornada em sua forma original no momento em que foi armazenada; É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas. Não pode ser confundido com confiabilidade do conteúdo (seu significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer integra (não sofrer alterações por pessoas não autorizadas).

Órgão Público – Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

Usuários – funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

5. Abrangência

Esta norma abrange a todos que utilizam de alguma forma os ativos de informação do Governo do Estado do Ceará.

6. 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 do Governo do Estado do Ceará.

7. Regras Gerais

- Os ativos tecnológicos (rede, sistemas, softwares, serviços de Internet, Correio Eletrônico, entre outros) são de propriedade do Governo do Estado do Ceará e deverão ser utilizados para realização do trabalho e interesses do Governo e da comunidade e serão administrados e monitorados pelo setor competente de TIC de cada órgão ou entidade estadual.
- As informações criadas, utilizadas e armazenadas nos equipamentos do Governo do Estado do Ceará são de propriedade do Governo e podem, quando necessário, serem acessadas pelo setor responsável de TIC, sendo, no entanto, preservada a sua integridade e confidencialidade.
- Equipamentos, tráfego de rede, softwares e sistemas podem ser auditados com objetivo de manutenção e segurança.

7.1. Inventário

- Todos os ativos devem ser identificados e documentados a sua importância.
- Todos os ativos devem possuir um responsável (proprietário), formalmente designado, que fará a correta classificação e acompanhamento periódico dos ativos.
- O inventário dos ativos deve conter as informações que ajudem a assegurar a sua proteção efetiva: nome do ativo, proprietário, custodiante, localização, cópia de segurança, criticidade, dentre outros específicos.
- A classificação quanto à criticidade obedecerá aos seguintes critérios:
  - Muito Alta – quando a interrupção do ativo provocar parada total das atividades.
  - Alta – quando a interrupção do ativo provocar perda de mais de 70% das atividades.
  - Média – quando a interrupção do ativo provocar perda entre 40 e 70% das atividades.
  - Baixa – quando a interrupção do ativo provocar perdas abaixo de 40% das atividades.

7.2. Proprietário e Custodiante

- Para todo Ativo da Informação do Governo do Estado do Ceará deverá ser designado um proprietário.
- O proprietário poderá delegar para um custodiante, mediante acordo formal, as tarefas de rotina diária daquele ativo, porém, a responsabilidade permanece com o proprietário.

7.3. Uso aceitável

- O uso da Internet e do correio eletrônico deverá basear-se conforme as normas NPS01 e NPS02 respectivamente.
- No que diz respeito ao uso de equipamentos computacionais:
  - Os computadores, notebooks e servidores são equipamentos fornecidos pelo Governo do Estado do Ceará devem ser utilizados para assuntos relativos ao trabalho do Governo.
  - As configurações padrão das estações de trabalho e servidores deverão ser estabelecidas e revisadas periodicamente pelo setor competente de TIC de cada órgão ou entidade estadual, e aprovadas pelo Comitê Gestor de Política de Segurança da Informação do Estado – CGSI.
  - Os servidores, computadores e notebooks devem estar protegidos com protetor de tela com ativação automática ou através de desconexão quando o usuário tiver que afastar-se do computador.
  - Os servidores, computadores e notebooks devem estar protegidos com software de detecção e reparo contra software/código maliciosos, com atualização sistemática.
  - Não será concedido o direito de administrador para os usuários de computador.
  - Arquivos com conteúdo importante, cuja perda represente prejuízo para o Governo do Estado do Ceará, devem ter cópia de segurança mantida em computador alternativo ou em um servidor, para fazer parte da rotina de backup.
  - Os equipamentos, principalmente os considerados críticos, devem estar instalados em áreas protegidas contra acessos indesejados.
  - Os equipamentos próprios, considerados de difícil reposição em função do custo financeiro, devem estar seguros, pelo menos contra incêndio.
  - Deverá ser instalado um sistema de nobreak e um gerador de energia próprio, que alimentem pelo menos os equipamentos e os locais considerados críticos.
  - No que diz respeito ao uso de Softwares e Sistemas:
  - A instalação de softwares e sistemas nos equipamentos computacionais do Governo do Estado do Ceará é de responsabilidade do setor competente de TIC de cada órgão ou entidade estadual.
  - Somente poderão ser instalados softwares e sistemas, pelo setor competente de TIC de cada órgão ou entidade estadual, com suas licenças de uso devidamente registradas.
  - No caso de instalação de softwares e sistemas nos equipamentos computacionais do Governo do Estado do Ceará, sem autorização devida, o usuário é responsável pela sua utilização, arcando com as penalidades e multas atribuídas.
  - O setor competente de TIC de cada órgão ou entidade estadual poderá realizar auditorias em computadores e notebooks para controlar a instalação indevida de softwares.
- No que diz respeito a Segurança Física e lógica:
  - Todas as áreas de TIC devem ser classificadas quanto à criticidade e à restrição de acesso e devem ser criados mecanismos para identificação e controle de acesso de pessoas que não desempenha suas funções no local.
  - Deverão ser criados mecanismos de controle acesso para funcionários do setor de TIC e não funcionários, em horários especiais, fora do expediente normal, indicando quem teve acesso, data e hora e quem autorizou.
  - As instalações prediais devem ser seguradas, pelo menos contra incêndio e quando aplicável uma sala cofre.
  - O cabeamento elétrico e lógico, que alimenta e interliga os vários equipamentos, deve ser protegido de forma adequada.
  - Devem ser criados mecanismos de proteção e combate a incêndio, principalmente em locais considerados críticos.
  - Devem ser planejados e implantados, quando aplicável, controles das condições ambientais.

7.4. Informação

- Toda informação produzida e armazenada pelo Governo do Estado do Ceará deverá receber um nível adequado de proteção, considerando a sua confidencialidade, integridade e disponibilidade, bem como qualquer outro requisito que seja considerado.
- Toda informação deverá ser classificada para indicar a sua criticidade, requisitos legais e sensibilidade.
- A classificação quanto ao sigilo obedecerá aos seguintes critérios:
  - Confidenciais – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar ao desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante os usuários externos.
  - Internas – informações de caráter setorial pertencentes a um órgão. O acesso a esse tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;
  - Secretas – informação crítica para as atividades do Governo do Estado do Ceará, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital.

- Públicas – informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal do Governo do Estado do Ceará, e cuja integridade não é vital;

- A classificação quanto à criticidade obedecerá aos seguintes critérios:
  - Muito Alta – quando a interrupção do ativo provocar parada total das atividades.
  - Alta – quando a interrupção do ativo provocar perda de mais de 70% das atividades.
  - Média – quando a interrupção do ativo provocar perda entre 40 e 70% das atividades.
  - Baixa – quando a interrupção do ativo provocar perdas abaixo de 40% das atividades.
- A troca de informações, softwares e sistemas entre órgãos do Governo do Estado do Ceará e entidades externas deverão ser realizadas de maneira formal.
- Se algum usuário souber sobre qualquer violação a esta Norma deverá comunicar ao Setor competente de TIC ou a sua chefia imediata.

9. Deveres, Responsabilidades e Recomendações

9. Deveres do Usuário

- O usuário não deverá:
  - Executar atividades que sejam ilegais, classificadas como crime ou contravenção, perante as leis locais, estaduais, federais ou internacionais enquanto utilizando os recursos computacionais sob o domínio do Governo do Estado do Ceará.
  - Copiar materiais protegidos por direito de cópia como digitalização e distribuição de fotografias e revistas, livros ou outras origens.
  - Utilizar os recursos computacionais do Governo do Estado do Ceará para obter ou transmitir materiais políticos, pornográficos, de pedofilia, ofensivos, segregatórios, discriminatórios e que violem leis de trabalho e raciais, entre outros.
  - Promover ou manter um negócio pessoal ou privado com oferta de produtos e/ou serviços, utilizando-se dos recursos computacionais e informações do Governo do Estado do Ceará, como base de operação e/ou de divulgação para ganhos pessoais.
  - Criar ou autorizar pontos de acesso.
  - Gerar interrupções na segurança da rede de comunicação.
  - Utilizar técnicas de obtenção de dados os quais os usuários estejam expressamente autorizados a acessar.
  - Realizar varredura na rede (port-scan ou sniffing), parada de serviços (DoS), roteamento falsificado e outros como inundação de pacotes (pinged floods), ou falsificação/ injeção de pacotes (packet spoofing) para propósitos maliciosos, a menos que estas obrigações estejam dentro do escopo de obrigações regulares.
  - Realizar varredura (busca) de portas (estrutura lógica que permite a comunicação entre computadores clientes e serviços oferecidos por computadores servidores).
  - Executar qualquer forma de monitoramento da rede que intercepte dados de usuários, a menos que esta atividade seja parte das obrigações ou função do usuário.
  - Executar atividades com intenção de enganar a autenticação do usuário ou segurança de qualquer serviço, computador, rede ou conta de qualquer organização, incluindo o uso de ferramentas de hardware ou software para remover/burlar a proteção de cópias de software, descobrir senhas, identificar vulnerabilidades de segurança, decodificar arquivos codificados, ou comprometer a segurança da informação por qualquer outro modo.
  - Executar quaisquer processos que envolvam suporte técnico, tais como abrir computadores ou mudá-los de localização, alteração nas configurações, instalação e desinstalação de recursos computacionais, exceto para usuários que têm essa atividade como função.
  - Utilizar programas/scripts/comandos, ou envio de mensagens de qualquer tipo, com a intenção de interferir ou desabilitar uma sessão autenticada de um usuário, através de qualquer meio, localmente ou via rede.
  - Apropriação ou cópia de arquivos eletrônicos sem permissão.
  - Visualização de arquivos e contas de outras pessoas, exceto no caso de tais atividades estarem dentro das obrigações da sua função.
  - Executar atividades não oficiais, tais como jogos eletrônicos, chats (bate- papo), programs P2P e Instant Messenger.
  - Escrever, copiar, executar, ou tentar introduzir qualquer código computacional designado para se auto-replicar, danificar, ou atrasar a performance de acesso para qualquer computador corporativo, rede ou informação.
  - Acessar outras redes usando modem ou outros mecanismos de acesso remoto sem a aprovação do setor de TIC.
  - Trazer descrédito para o Governo do Estado do Ceará, seus parceiros e colaboradores.
  - Revelar, sem autorização, qualquer informação do Governo do Estado do Ceará que não seja pública.
  - Desativar, em hipótese alguma, o software de detecção e reparo de software/código malicioso.
  - Abrir anexos que contenham arquivos executáveis (.exe, .pif, vbs, entre outros). Exceção - Somente poderão ser abertos esses tipos de anexos se o usuário conhecer a fonte e o estiver esperando.
  - Reinicializar seus equipamentos por meio de disquetes ou cd-roms, não importando a sua origem.

9.2. Responsabilidades do Usuário

- Comunicar ao setor competente de TIC do órgão ou entidade estadual qualquer evento com software/código malicioso ou problemas que venham a ocorrer envolvendo os recursos computacionais ao qual esteja utilizando.
- Zelar pelo fiel cumprimento ao estabelecido nesta Norma.

9.3. Responsabilidades do Setor de TIC

- Instalar e atualizar regularmente o software de detecção e reparo contra software/código malicioso, em estações de trabalho e servidores.
- Instalar as correções de segurança nos softwares sempre que necessário.
- Definir e atualizar os procedimentos de gerenciamento e a atribuição de responsabilidades no que diz respeito à proteção contra software/código malicioso, treinamento em seu uso, comunicação de incidentes e procedimentos de recuperação contra ataques;
- Manter um plano de continuidade operacional dos serviços caso ocorra algum evento relacionado com segurança.
- Manter um plano de continuidade contra ataques, incluindo os procedimentos quanto a utilização de cópias de segurança de dados e softwares, hardware adicional e outras.
- Adotar mecanismos para verificação automática de software/ código malicioso nos servidores de correio eletrônico e estações de trabalho.
- Determinar, quando necessário, a possibilidade de barrar anexos utilizados tipicamente como vetores de software/ código malicioso, antes de sua entrada na rede ou no servidor de correio, por meio de ferramentas de controle e encaminhamento de e-mail (relay).
- Registrar e armazenar todos os eventos referentes a detecção e controle contra software/código malicioso por um período mínimo de 1 (uma) semana.

10. 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.

NORMA NPS06

CONTINGÊNCIA E CONTINUIDADE DO NEGÓCIO

1. Apresentação

Considerando a necessidade de continuidade dos negócios do Governo do Estado do Ceará é de grande importância a definição e implementação de procedimentos formais de gestão, de forma a reduzir riscos, limitar as conseqüências aos danos de incidentes e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

2. Objetivo

Estabelecer os procedimentos adequados para montagem do plano de contingência adequado para os elementos que impactam diretamente no ambiente de Tecnologia da Informação e Comunicação (TIC) do Governo do Estado do Ceará, garantindo a continuidade dos negócios, quando houver algum tipo de interrupção nos ativos críticos do Governo.

3. Documentos de referência

Diretrizes da Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará.

4. Definições

Ativo – Qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004]

Ativos de Informação – Bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisas, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas. [ISSO/IEC 13335-1:2004];

- Ativos de Software – Aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.
- Ativos Físicos – equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos.
- Ativos Serviços – serviços de computação e comunicações, utilidades gerais, por exemplo: aquecimento, iluminação, eletricidade e refrigeração.

Incidente – eventos indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Complexão – Conjunto, união, encadeamento, concatenação.

Mirror – Uma cópia exata de um conjunto de dados.

Patches – programa criado para atualizar ou corrigir um software.

Mídia de Armazenamento – Suporte no qual pode se registrar a informação digital, como por exemplos: fitas magnéticas, disquetes, discos ópticos.

Órgão Público – Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

Usuários – Funcionários, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

5. Abrangência

Esta norma abrange a toda a infra-estrutura tecnológica do Governo do Estado do Ceará.

6. 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 do Governo do Estado do Ceará.

7. Regras Gerais

- Os processos críticos do negócio dos órgãos e entidades do Governo do Estado do Ceará devem ser identificados e categorizados quanto a sua criticidade.
- Deverão ser planejados e elaborados planos de continuidade para cada ameaça considerada, em cada um dos processos críticos do negócio, definindo em detalhes os procedimentos a serem executados em estado de contingência.
- Os planos de continuidade deverão contemplar a Administração da Crise que deve definir passo-a-passo o funcionamento das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade, a Continuidade Operacional que definirá os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, conseqüentemente, os impactos potenciais ao negócio e a Recuperação de Desastres que contemplará um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação.
- Devem ser elaborados planos de continuidade para, no mínimo, as situações:
  - Perda de áreas críticas, como CPD;
  - Perda de equipamentos críticos, como servidores, ativos de rede;
  - Parada de sistemas operacionais;
  - Parada de softwares de apoio considerados críticos;
  - Parada de softwares aplicativos considerados críticos;
  - Greve de pessoal
- Todos os ativos envolvidos em processos críticos do órgão e entidade de TIC devem ser identificados e categorizados quanto a sua criticidade da seguinte forma:
  - Apresentar os itens a serem avaliados, ou seja, os ativos e os seus processos para os envolvidos;
  - Cada envolvido deverá atribuir valores de 01 a 05 para cada item considerado, utilizando o formulário padrão para estabelecer a criticidade (PSFOR01), em anexo:
    - A influência do item em termos de sua gravidade (G), urgência (U) e tendência (T) de agravamento;
    - A abrangência (A) do ativo sobre o órgão ou entidade do Governo;
  - Após a atribuição dos valores para cada item, pelos envolvidos no processo de avaliação, deve-se multiplicar o valor da gravidade, urgência, tendência e abrangência (GxUxTxA).

    Quanto maior o valor obtido, maior a prioridade do item.

NORMA NPS06

CONTINGÊNCIA E CONTINUIDADE DO NEGÓCIO

□ Tabela de pontuação referente a criticidade

Identificação do Ativo

Valor	Gravidade	Urgência	Tendência	Abrangência	Total
5	Os prejuízos ou dificuldades são extremamente graves	É necessário uma ação imediata.	Se nada for feito a situação irá piorar rapidamente	O ativo tem impacto sobre todo o órgão/entidade	625
4	Muito graves	Urgente	Vai piorar em pouco tempo	O impacto incide sobre todo o órgão/entidade	256
3	Graves	Tão cedo quanto possível	Vai piorar a médio prazo	Atinge parte do o órgão/entidade	81
2	Pouco graves	Pode esperar um pouco	Vai piorar a longo prazo	Restringe-se a um setor/departament o	16
1	Sem gravidade	Não tem pressa	Não vai piorar e pode até esperar	Rede Local	1

□ A avaliação dos resultados deve ser considerada da seguinte forma:

- Pontuação entre 256 e 625: ativos em que devem se concentrar as atenções e esforços quanto à segurança e providências quando ocorre alguma falha;
- Pontuação entre 81 e 256: ativos que merecem atenção especial, mas depois de atendidas as necessidades dos pontuados acima desta faixa;
- Pontuação abaixo de 81: ativos que não oferecem grandes prejuízos quando em situação de falha.

- Todo sistema que deve possuir procedimentos alternativos (manuais) independentes do fluxo normal do sistema para aqueles processos que forem qualificados como críticos por demandarem ônus para o Governo do Estado do Ceará.
- Deverão ser realizados testes a intervalos regulares em todos os níveis de contingência implantados.

8. Recomendações

8.1. – Quando do tratamento de incidentes de segurança da informação deverão ser adotadas as seguintes ações:

- Definir as metas e objetivos no tratamento de um incidente;
- Identificar quem deverá ser contatado no caso de um incidente, como gerentes, pessoal dos locais afetados, grupos responsáveis por segurança, etc.;
- Identificar se o incidente é realmente um incidente e o seu grau de seriedade;
- Definir o que será feito na ocorrência de um incidente, como notificar os interessados, proteger as evidências e conservar os registros, durante e depois do incidente (logs das atividades);
- Identificar como o dano deve pode ser limitado;
- Eliminar as causas do incidente;
- Restabelecer o serviço ou sistemas;
- Verificar quais as implicações do incidente passado;
- Resposta administrativa para o incidente, ou seja, baseado na política de segurança verificar que ações deverão ser adotadas no caso do incidente haver sido provocado por um usuário. (sanções adequadas).

8.2 – Na contingência média é aceitável a disponibilidade em horário comercial, podendo ser interrompida eventualmente.

➢ Contingência para Servidores

- Procedimentos de Backup diários, baseados em cronograma

e íntegros de forma que a recuperação dos dados possa ser realizada de forma segura e em qualquer momento, verificando periodicamente a correção e a complexão;
- Contrato de manutenção de Hardware 5x8 (Segunda a sexta-feira x oito horas por dia);
- Na falta de contrato de manutenção, possuir peças de reposição e pessoal técnico para solucionar o problema;
- Manutenção de patches atualizados;
- Disco de boot espelhado (mirror).

➢ Contingência para outros Ativos de Rede
- Contrato de manutenção de Hardware 5x8 (Segunda a sexta-feira x oito horas por dia) e/ou elemento de backup;
- Na falta de contrato de manutenção, possuir hardware de backup e pessoal técnico para solucionar o problema;

8.3 – Na Contingência Alta é requerida disponibilidade 7x24 (segunda-feira a domingo x 24 horas), podendo ser interrompida eventualmente.

➢ Contingência para Servidores
- Procedimentos de Backup diários, baseados em cronograma e íntegros de forma que a recuperação dos dados possa ser realizada de forma segura e em qualquer momento, verificando periodicamente a correção e a complexão;
- Cópia de segurança armazenada em 2 tipos diferentes de mídia;
- Contrato de manutenção de hardware 7x24 (segunda-feira a domingo x 24 horas);
- Na falta do contrato de manutenção, possuir outro hardware idêntico e pessoal técnico em regime de plantão;
- Manutenção de patches atualizados;
- Todos os discos espelhados;
- Placas de rede redundantes;
- Utilização de nobreaks;

➢ Contingência para outros Ativos de Rede
- Contrato de manutenção de hardware 7x24 (segunda-feira a domingo x 24 horas);
- Na falta do contrato de manutenção, possuir outro hardware idêntico e pessoal técnico em regime de plantão;
- Alimentação através de nobreaks;

8.4 – Na Contingência Altíssima é requerida disponibilidade 7x24 (segunda-feira a domingo x 24 horas) sem interrupções.

➢ Contingência para Servidores
- Procedimentos de Backup diários, baseados em cronograma e íntegros de forma que a recuperação dos dados possa ser realizada de forma segura e em qualquer momento, verificando periodicamente a correção e a complexão;
- Cópia de segurança armazenada em 2 tipos diferentes de mídia de armazenamento;
- Armazenamento das mídias de backup em local físico alternativo;
- Contrato de manutenção de hardware 7x24 (segunda-feira a domingo x 24 horas);
- Manutenção de patches atualizados;
- Todos os discos espelhados;
- Placas de rede redundantes;
- Fontes de alimentação do hardware redundantes;
- Utilização de Grupo gerador e nobreaks;
- Hardware idêntico em espera (Standby) com Failureover automatizado por serviço;
- Ambiente alternativo em local físico diferente do principal, cujo tempo de disponibilização por serviço não ultrapasse 8 horas;
- Pessoal técnico distribuído em plantão.

➢ Contingência para outros Ativos de Rede
- Contrato de manutenção de hardware 7x24 (segunda-feira a domingo x 24 horas);
- Pessoal técnico distribuído em plantão;
- Hardware com fonte redundante;
- Hardware idêntico em espera (Standby) utilizando protocolo VRRS no caso de roteadores;
- Utilização de grupo gerador e nobreaks.

9. 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.

10. Anexo

10.1. PSFOR01 – Formulário padrão para estabelecer a criticidade dos ativos.

GOVERNO DO ESTADO DO CEARÁ	Política de Segurança dos Ambientes de TIC do Governo do Estado do Ceará	Versão	Dt Avaliação	Página
		1.0		1/1

PSFOR01

FORMULÁRIO PARA ESTABELECER CRITICIDADE DOS ATIVOS

Ativo				Importância para o Negócio				Total Pontos (GxUxTxA)
Identificador	Descrição	Nome Responsável	Localização	Gravidade	Urgência	Tendência	Abrangência	

Data da avaliação: ___/___/_____

Nome e assinatura do(s) avaliador(es):_____