GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Controle e Transparência

Subsecretaria de Estado da Transparência

Laboratório de Dados, Análise e Tecnologia Aplicada à Auditoria-
LAB.DATA

Política de Segurança da Informação

3ª Edição

Vitória, Outubro 2019

.

SECRETARIA DE ESTADO DE CONTROLE E TRANSPARÊNCIA – SECONT

Edmar Moreira Camata
Secretário de Estado de Controle e Transparência

Marcelo Campos Antunes
Subsecretário de Estado de Controle

Mirian Porto do Sacramento
Subsecretário de Estado da Transparência

Marcelo Martins Altoé
Subsecretário de Estado de Integridade Governamental e Empresarial

Helmut Mutiz D'Auvila
Corregedor Geral do Estado

NEGÓCIO
Controle interno da administração pública e da gestão dos recursos públicos estaduais.

MISSÃO
Assegurar a efetiva e regular gestão dos recursos públicos, em benefício da sociedade.

VISÃO
Ser instituição de excelência no controle e contribuir para o aperfeiçoamento da Administração Pública.

GOVERNO DO ESTADO DO ESPÍRITO SANTO

Secretaria de Estado de Controle e Transparência

Política de Segurança da Informação

3ª Edição

Versão inicial: Marcos dos Santos Ferreira, Carlos Santana Bandeira, Eduardo Stavich, Emerson Couto de Moura, Fernanda Barcellos Tommasi Finamore Simoni e Ricardo Monteiro Oliveira

Revisão : Carlos Santana Bandeira, Emerson Couto de Moura, Fabiano da Rocha Louzada e Mirian Porto Sacramento

Vitória, setembro de 2019

Apresentação

A preocupação com a segurança da informação e, mais especificamente, com o tratamento dado as informações mantidas pelos órgãos públicos tem crescido na medida em que se consolida a percepção de que, cada vez mais, dependemos destas informações para a continuidade de nossas atividades.

A informação é elemento essencial para todos os processos de negócios dentro de uma organização, sendo, portanto, um bem ou um ativo de grande valor, podendo ser alvo de uma série de ameaças com a finalidade de explorar vulnerabilidades e obter lucro, ou simplesmente causar prejuízos.

Portanto, faz-se necessária a implantação de políticas de segurança de informação que busquem reduzir as chances de fraudes, perda de informações ou resguardas a instituição e seus servidores de questionamentos judiciais.

O Governo do Estado do Espírito Santo, Através do Decreto nº 2884-R, de 21 de outubro de 2011, instituiu a Política de Segurança da informação no âmbito do poder Executivo do ES.

Diferentemente das secretarias e outros órgãos (SEDU, SESP, SESA, etc.) onde a gerência de informação é uma atividade de apoio a sua missão final, na SECONT gerenciar informações constitui a própria essência de suas atividades. É indiscutível, portanto, a relevância que devemos atribuir aos processos que busquem aplicar e aprimorar a gestão da segurança da informação.

A segurança da informação busca proteger a SECONT de um grande número de ameaças no intuito de assegurar sua credibilidade como mantenedora de informações corporativas. Esta segurança é obtida a partir da utilização de uma série de controles, que podem ser políticas, práticas e procedimentos, os quais precisam ser estabelecidos para garantir que objetivos de segurança específicos sejam atendidos.

Uma política de segurança é o documento mais importante em nosso Sistema de Gerenciamento da Segurança da Informação, seu objetivo é implantar métodos e procedimentos que devem ser de conhecimento de todos os servidores, quer sejam

efetivos, cedidos, comissionados, estagiários ou que tenham qualquer outro vínculo temporário ou definitivo com esta instituição.

Os controles de segurança, de um modo geral, são definidos para garantir um nível de segurança coerente com as atividades exercidas e, a partir destes, serão definidos nossa política de uso aceitável dos recursos tecnológicos.

Nossa intenção não é impor restrições contrárias à cultura de abertura e confiança da SECONT, mas proteger o órgão, nossos servidores e parceiros de ações ilegais ou danosas praticadas por qualquer indivíduo, de forma proposital ou inadvertidamente.

As regras e procedimentos definidos nesta Política de Segurança devem ser seguidos para a garantia da segurança da informação.

Qualquer violação será passível de investigação e, se for o caso, aplicação de sanções disciplinares.

A partir de sua divulgação a todos os servidores da SECONT, não será admitida a alegação de seu desconhecimento.

É importante que as informações da política de segurança sejam divulgadas para todos os servidores da SECONT e que todos estejam conscientes de sua importância.

ÍNDICE

I. Introdução 6
II. Diretrizes Gerais 9
III. Normas Para Utilização da Internet 13
IV. Normas para Utilização de Correio Eletrônico 17
V. Normas para Utilização da Rede Local 21
VI. Normas para Classificação de Documentos Eletrônicos 26
VII. Normas para Gestão de Ativos 32
VIII. Normas para Utilização de Conta e Senha dos Usuários 41
IX. Normas para Utilização de Conta e Senha dos Administradores 46
X. Normas para Utilização do Sistema de Mensagens Internas 50
XI. Normas Gerais para Manuseio de Processos ou Quaisquer Outros Documentos Tramitados na SECONT 53
XII. Modelo do Termo Individual de Responsabilidade 54
XIII. Modelo do Termo Individual de Confidencialidade 56
XIV. Glossário 57

I. INTRODUÇÃO

O objetivo de uma política de segurança da informação é garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade das informações produzidas na empresa ou por ela custodiada, assim como permitir que as mesmas sejam auditadas a qualquer tempo.

A informação deve ser compreendida como um bem da organização, um dos recursos críticos para a realização das atividades da secretaria e, portanto, possui grande valor e deve SEMPRE, ser tratada profissionalmente, com responsabilidade e isenção.

Todo e qualquer usuário de recursos computadorizados da SECONT tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

A Política de segurança da informação na SECONT, doravante denominada apenas PSI/SECONT, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento de dados ou que tenha acesso a informações da Secretaria.

Entende-se como violação desta PSI, qualquer ato que:

- Exponha a SECONT a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados, informações ou perda de equipamentos.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Este documento procura contemplar as diretrizes da PSI/SECONT consoante às diretrizes da Política Estadual de Segurança da Informação abrangendo os temas descritos no Art. 3º, parágrafo único do Decreto 2884 de 21/10/2011, quais sejam:

I. propriedade;
II. responsabilidade;
III. acesso;
IV. classificação da Informação;
V. auditoria e conformidade;
VI. gestão de riscos;
VII. gestão da continuidade;
VIII. conscientização do agente público;
IX. comprometimento, violação e sanções;
X. divulgação e atualização.

A Política de Segurança da Informação da SECONT é composta por 3 (três) tipos de documentos, a saber:

a. **Diretrizes Gerais** - São as regras de alto nível que representam os princípios básicos que a SECONT resolveu incorporar à sua gestão de acordo com a visão estratégica de sua direção. Servem como base para que as normas e os procedimentos sejam criados e detalhados.

b. **Normas** - Especificam no plano tático as escolhas tecnológicas, regras de utilização e os controles que devem ser utilizados para que se efetive a estratégia definida nas Diretrizes Gerais.

c. **Instruções e Procedimentos** - Detalham no plano operacional as configurações de um determinado produto ou sistema que deve ser feita para implantar os controles e tecnologias estabelecidas nas Normas.

II. DIRETRIZES GERAIS

2.1. Diretrizes gerais para a segurança da informação e para o uso aceitável da infraestrutura tecnológica da SECONT, visando preservar a integridade, confidencialidade e disponibilidade das informações sob sua gestão, bem como a autenticidade da identidade de quem as acessa.

a. A SECONT elaborará e aplicará o conjunto de normas e procedimentos necessários à operacionalização das diretrizes descritas pela sua Política de Segurança da Informação.

b. A PSI/SECONT se aplica às informações sob gestão desta Secretaria em qualquer modalidade: escrita em papel, imagens, vídeos ou arquivos de som, obtidos, armazenados ou transmitida por meios eletrônicos, exibida em filmes ou falada em conversas formais e informais. Em suma, seja qual for a forma ou o meio através do qual a informação possa ser exibida ou compartilhada, ela sempre deverá ser protegida adequadamente, de acordo com os controles definidos pela presente política.

c. A PSI/SECONT deve ser conhecida e obedecida por todos os servidores da Secretaria, quer sejam efetivos, temporários, comissionados ou terceirizados, sendo de responsabilidade de cada um o seu cumprimento. A política está disponível integralmente em documento eletrônico na pasta “DIVERSOS/PSI”.

d. No âmbito da SECONT, é permitido aos usuários somente a utilização de recursos de processamento e armazenamento de informação que estejam formalmente homologados pelo órgão, permitindo garantir que os requisitos de segurança sejam atendidos. Cabe aos chefes de setor, coordenadores e subsecretários tomarem as medidas cabíveis para a concessão e cancelamento do acesso aos recursos necessários.

e. Somente atividades lícitas, éticas, morais e administrativamente admitidas devem ser realizadas, pelos usuários, quando da utilização dos recursos de processamento e armazenamento de informação da

SECONT, ficando os transgressores sujeitos às sanções previstas nestas diretrizes.

f. O acesso externo à internet, quer seja para navegação ou qualquer outro serviço disponibilizado (Whatsapp, Instagram etc..), quando concedido, deverá prezar pela lisura e boa conduta aqui descritas, evitando fazer comentários em redes sociais, enviar mensagens eletrônicas, enfim, praticar qualquer ato de cunho pessoal utilizando os links de dados oficiais desta instituição.

g. Os documentos produzidos na utilização dos recursos de processamento de informação da SECONT são de propriedade da Administração Pública Estadual. De igual modo, os programas e serviços desenvolvidos ou implantados por servidores do quadro efetivo, comissionado ou prestadores de serviço.

h. As informações de propriedade ou custodiadas pela SECONT devem ser utilizadas apenas para os propósitos definidos pela sua atuação institucional. É vedado aos usuários, em qualquer tempo ou sob qualquer propósito, apropriarem-se dessas informações.

i. A identificação do usuário (por meio de nome e senha ou qualquer outro modo) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo pré-requisito para a utilização dos recursos de TI o preenchimento do Termo Individual de Responsabilidade, que deve indicar as condições de uso e seus direitos e deveres.

j. Todos os servidores, efetivos, comissionados, cedidos, estagiários e qualquer outro que esteja prestando serviços na SECONT devem assinar o Termo Individual de Responsabilidade e o Termo Individual de Confidencialidade, sem o qual não poderá ter acesso às informações protegidas por esta Política de Segurança da Informação.

k. A SECONT se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicações, incluindo o acesso à internet, o sistema de troca de mensagens internas, o uso do correio eletrônico institucional, a utilização das impressoras e a utilização de arquivos e programas.

l. Os recursos tecnológicos de processamento e armazenamento de informação que forem disponibilizados aos usuários serão previamente definidos em projetos que indiquem claramente o seu escopo de utilização, a fim de evitar situações de risco à segurança da informação. Antes de serem colocados em produção, serão testados em ambiente de homologação.

m. Todos os documentos eletrônicos gerados ou custodiados pela SECONT são em princípio considerados como privativos do órgão e a sua classificação quanto ao seu nível de confidencialidade, bem como o encaminhamento e distribuição serão regulados pela autoridade competente designada para isto.

n. Todos os usuários, ao tomarem conhecimento de qualquer incidente de segurança da informação, devem notificar o fato, imediatamente, à Coordenação de Tecnologia da Informação, através de e-mail (*security_officer@secont.es.gov.br*) ou através de comunicação interna.

De acordo com as diretrizes estabelecidas ficam vedadas as seguintes práticas no ambiente da SECONT:

I. Armazenar imagens, áudio ou vídeo que não sejam por nós produzidos de forma oficial ou que tenhamos, legalmente, direitos de propriedade nos equipamentos da SECONT.

II. Utilizar a infraestrutura física ou os recursos tecnológicos da SECONT para trabalhos particulares, quer seja para si ou para outrem;

III. Divulgar ou distribuir, qualquer conteúdo de informação produzido pela SECONT, ainda que classificado como acesso público, sem o consentimento da autoridade competente para sua divulgação;

IV. Distribuir, divulgar, compartilhar ou conceder acesso a informações de outras entidades, custodiadas pela SECONT, sem o conhecimento e aceite do proprietário dos dados, ainda que classificado como de acesso público.

V. Retirar quaisquer documentos produzidos ou em trâmite na SECONT, para manuseio em domicílio, escritório ou qualquer outro ambiente particular.

VI. Praticar qualquer ato ilegal, imoral ou que atente contra a imagem da Instituição, ainda que de maneira subjetiva.

A não observância dos preceitos desta política implicará na aplicação de sanções administrativas, cíveis e penais previstas em lei ou em qualquer outra legislação que venha regular a matéria.

III. NORMAS PARA UTILIZAÇÃO DA INTERNET

OBJETIVO

Estabelecer responsabilidades e requisitos básicos para utilização da Internet no ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

ABRANGÊNCIA

Esta norma se aplica a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação (TIC) da SECONT para acesso à Internet, por qualquer via (links oficiais, conexões de celular 3G, 4G, SMS ou qualquer outro concedido pela instituição).

CONCEITO

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de utilizarem seus recursos.

Considerando que o uso da Internet, no âmbito da SECONT, constitui uma concessão e não um direito é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada deste importante recurso tecnológico.

Todos os usuários dos ativos de informação de propriedade ou controlados pela SECONT, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

UTILIZAÇÃO DA INTERNET

1. A utilização da internet através de conexões disponibilizadas pela SECONT é uma concessão que a Secretaria disponibiliza para o bom desempenho de seus funcionários e, portanto, deverá ser utilizada exclusivamente para atividades relacionadas aos objetivos institucionais do órgão, sempre em conformidade com a lei, e com respeito à moral e aos bons costumes e a ordem pública.
2. A infraestrutura de tecnologia da SECONT possui mecanismos de autenticação que determinam e registram a titularidade dos acessos à Internet realizados por seus usuários.
3. É expressamente proibido:
    a) Divulgar informações institucionais quer sejam sigilosas ou não, em listas de discussão, bate-papo, redes sociais e/ou qualquer outro meio de conhecimento público.
    b) Copiar qualquer software licenciado para a SECONT, ou informações de propriedade e/ou custodiada por ela sem a autorização expressa da direção do órgão ou do responsável pelo software/informação.
    c) Fazer *download* de arquivos da Internet que permitam a instalação de programas ou sistemas sem a intervenção do setor de Suporte Técnico.
    d) Utilizar-se de "*modem*", ou qualquer dispositivo de compartilhamento em máquinas que estejam conectadas ao ambiente da rede da SECONT sem o consentimento e autorização expressa do Secretário ou do responsável por ele designado.
    e) Uso de *softwares* de comunicação instantânea, tais como *ICQ*, *Microsoft Messenger* (*MSN*), skype e afins, a não ser por autorização expressa do Secretário de Estado de Controle e Transparência e para período e fins por ele estabelecidos.

f) Utilização de softwares *peer-to-peer* (*P2P*), tais como *Kazaa*, *Emule, Bot Torrent* e afins.

g) Não é permitido o acesso a sites de relacionamento, tais como Facebook, *MySpace, WatsAppWeb* e afins ou a qualquer site de *Proxy*.

4. Periodicamente serão gerados relatórios dos sites acessados pelos usuários da SECONT. A direção do órgão terá acesso a essas informações a qualquer tempo.
5. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso (nome de usuário e senha).
6. Os usuários que desejarem utilizar outras conexões, além daquelas já estabelecidas, deverão obrigatoriamente informar ao setor de suporte ou ao responsável pela Segurança da Informação da SECONT.
7. Será de responsabilidade de cada usuário zelar pelo fiel cumprimento do estabelecido pela presente norma.
8. A SECONT monitora e bloqueia automaticamente sites de pornografia e contrários à lei, porém, mesmo que ocorram falhas na segurança e sites com este conteúdo estejam liberados, o acesso a estes constituem violação às regras aqui estabelecidas, cabendo ao usuário relatar ao setor de suporte a ocorrência de comportamento anormal do Browser (Software navegador).
9. A não observância de qualquer item acima implicará nas sanções previstas nesta norma.

SANÇÕES

De acordo com as diretrizes gerais desta política de segurança da informação, a SECONT se reserva o direito de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet.

A verificação do cumprimento das **Normas para Utilização da Internet** será efetuada da seguinte forma:

1. Os servidores do Setor de Suporte Técnico identificarão os usuários que violarem qualquer item da presente norma de segurança.
2. As transgressões das normas estabelecidas neste documento serão comunicadas ao Chefe de Segurança de informação (Chief Security Officer) que identificará a gravidade da situação e noticiará o transgressor, ao Secretário de Estado de Controle e Transparência e ao Coordenador/Chefe da área.
3. O transgressor está sujeito às sanções administrativas tais como advertência, suspenção e processo administrativo com vistas a apuração da gravidade do ato praticado além de ser responsabilizado civilmente caso a transgressão se caracterize como crime ou contravenção penal.
4. Independentemente das ações administrativas, os direitos de acesso podem ser revogados, a critério do Secretário ou por determinação do Chefe de Segurança da Informação.

IV. NORMAS PARA UTILIZAÇÃO DE CORREIO ELETRÔNICO

OBJETIVO

Estabelecer responsabilidades e requisitos básicos para uso dos serviços de Correio Eletrônico (e-mail) no ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

ABRANGÊNCIA

Esta norma se aplica a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação (TIC) da SECONT para acesso as funcionalidades do Correio Eletrônico.

CONCEITO

Grande parte das comunicações diárias da SECONT é recebida através de e-mail. Porém, devemos sempre lembrar que a maioria das pragas eletrônicas atuais (vírus, trojans, spyware, etc.) também chega por esse meio. Estas pragas eletrônicas podem ser enviadas automaticamente, isso significa que um e-mail de um contato comercial, de outro servidor público ou de um amigo não foi mandado necessariamente pelo mesmo.

Nossos servidores de e-mail encontram-se protegidos contra ameaças eletrônicas diversas, mas algumas atitudes do usuário final são importantes. A facilidade de correio eletrônico fornecida pela SECONT deve ser usada exclusivamente no interesse do serviço.

Considerando que o uso dos serviços de Correio Eletrônico no âmbito da SECONT 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 dos ativos de informação de propriedade ou custodiados pela SECONT, ao utilizarem esse recurso, deverão fazê-lo no estrito interesse do órgão, mantendo uma conduta profissional especialmente em se tratando da utilização de bem público.

UTILIZAÇÃO DO CORREIO ELETRÔNICO

A SECONT se reserva o direito de verificar, sempre que julgar necessário, a obediência às normas citadas neste documento. Esta verificação será realizada através da análise do conteúdo das mensagens dos e-mails e de seus anexos e através de análises técnicas de seu envio e/ou recebimento.

1. Todas as contas de correio eletrônico fornecidas pela instituição terão uma titularidade, determinando-se desta forma a responsabilidade sobre sua utilização.
2. Os usuários da SECONT serão titulares de uma única caixa postal individual no servidor de correio eletrônico, com direito de envio e recebimento de mensagens enquanto perdurar o seu vínculo com o órgão.
3. Embora os usuários sejam titulares da conta, estes não são proprietários, a conta de e-mail é uma concessão e pode ser monitorada, ou auditada a qualquer tempo por decisão do Secretário;
4. As contas de e-mail com inatividade por um período igual ou superior a 90 (noventa) dias serão bloqueadas.
5. As contas de e-mail dos servidores aposentados permanecerão ativas por um período máximo de 60 dias, após o que serão bloqueadas
6. O tamanho das caixas postais, limites de mensagens e quantidade de endereços por mensagens serão disponibilizados de acordo com a infraestrutura suportada pelo PRODEST.
7. O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico.
8. O Setor de Suporte Técnico é responsável pela inclusão, exclusão e alteração dos usuários de correio eletrônico da SECONT.

9. É vedada a utilização do correio eletrônico para as seguintes situações:

    a. Enviar mensagens não autorizadas divulgando informações sigilosas de propriedade do Governo.

    b. Acessar a caixa postal de outro usuário sem autorização formal do mesmo.

    c. Acessar o banco de dados do correio eletrônico de outro órgão sem autorização formal.

    d. Utilizar contas de e-mail particulares seja através de *webmail* ou dos serviços *Post Office Protocol (POP)*, *Internet Message Access Protocol (IMAP)* e *Simple Mail Transfer Protocol (SMTP)* de provedores não pertinentes ao domínio *es.gov.br em comunicações oficiais sem o conhecimento do Secretário de Estado de Controle e Transparência* .

    e. Enviar, armazenar ou manusear material que caracterize a divulgação, incentivo ou prática de atos 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 da SECONT, bem como as informações neles mantidas.

    f. Enviar, armazenar ou 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 para assuntos pessoais ou privados.

    g. Envio de mensagens do tipo "*corrente*" e "*spam*".

    h. Envio intencional de mensagens que contenham vírus eletrônicos ou qualquer forma de rotina de programação de computador prejudicial ou danosa.

i. Envio de mensagens que contenham arquivos com código executável *(.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf*, etc.) ou qualquer outra extensão que represente um risco à segurança, de acordo com os critérios estabelecidos pela Coordenação de Tecnologia da Informação.

j. Utilização de listas e/ou caderno de endereços da SECONT ou de qualquer outro órgão da administração estadual 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.

k. Todo e qualquer procedimento de uso do correio eletrônico, não previsto nesta norma, que possa afetar de forma negativa a SECONT ou ao Governo.

10. As exceções serão tratadas pelo responsável pela segurança da informação.

SANÇÕES

De acordo com as diretrizes gerais desta política de segurança da informação, a SECONT se reserva o direito de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo o envio e recebimento de e-mail.

A verificação do cumprimento das **Normas para Utilização do E-mail** será efetuada da seguinte forma:

1. Os servidores do Setor de Suporte Técnico identificarão os usuários - doravante chamados de infratores - que violarem qualquer item da presente norma de segurança.

2. As transgressões das normas estabelecidas neste documento serão comunicadas ao infrator, ao seu superior imediato e ao Secretário de Estado de Controle e Transparência conforme a gravidade da infração.

3. Caso a transgressão caracterize crime ou contravenção penal, será apresentada *notitia criminis* à Polícia Judiciária, sem prejuízo das sanções administrativas e cíveis cabíveis.

V. NORMAS PARA UTILIZAÇÃO DA REDE LOCAL

OBJETIVO

Estabelecer responsabilidades e requisitos básicos para a utilização da Rede Local no ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

ABRANGÊNCIA

Esta norma se aplica a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação (TIC) da SECONT para acesso à sua Rede Local.

CONCEITO

A Rede Local da SECONT é uma estrutura composta por diversos ativos de TI, entre eles podemos destacar: estações de trabalho (*desktops*), *notebooks*, cabeamento estruturado, servidores de arquivos, impressoras, *switches*, *roteadores*, etc.

Alguns destes ativos são as principais ferramentas utilizadas pelos usuários na criação, no armazenamento e na manipulação das informações produzidas ou custodiadas pela SECONT. A definição de regras e boas práticas de utilização destes ativos constitui fator primordial à segurança da informação.

Considerando que o uso da Rede Local, no âmbito da SECONT, constitui uma concessão e não um direito é de extrema importância que sua utilização (gravação de arquivos, impressão, etc.) corresponda ao interesse público e ao estabelecido na presente norma.

UTILIZAÇÃO DA REDE LOCAL

1. As tentativas de obtenção de acesso não autorizado, tais como fraudar a autenticação de usuário ou a segurança de qualquer servidor de dados, rede ou conta, obter acesso a dados não disponíveis para o usuário, conectar-se ao servidor de dados ou conta cujo acesso não seja expressamente autorizado ou colocar à prova a segurança de outras redes

serão severamente repreendidas e o servidor poderá ser punido de acordo com a gravidade da infração.

2. Não são permitidas interferências nos serviços de qualquer outro usuário, servidor de dados ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor de dados e procedimentos que busquem violar a segurança de um servidor de dados.

3. Antes de ausentar-se do seu local de trabalho, o usuário deverá efetuar o procedimento de *logoff* da rede ou o bloqueio de sua estação de trabalho ou notebook.

4. O usuário deverá fazer manutenção periódica nas suas pastas pessoais, evitando acúmulo de arquivos desnecessários.

5. Qualquer material de natureza pornográfica, racista ou que possa ser entendido como preconceituoso, ainda que de forma não explícita, não poderá ser exposto, armazenado, distribuído ou editado através do uso dos recursos da Rede Local.

6. Não é permitido manter arquivos fora das áreas de armazenamento destinadas aos usuários, de forma que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento, no servidor de arquivos, são designadas conforme mostra a tabela abaixo:

Compartilhamento	Utilização
(Z:) Pastas Pessoais	• Nesta pasta devem ser armazenados os arquivos de responsabilidade do proprietário da pasta. Somente o proprietário e os administradores da Rede Local conseguem acessar e manipular os arquivos armazenados. • Esta pasta deve ser utilizada, preferencialmente, no armazenamento de documentos ainda em fase de elaboração e na guarda de arquivos de manipulação exclusiva

	do usuário, mantendo-se o interesse institucional de seu armazenamento.
(Y:) Pastas Departamentais	• Nesta pasta devem ser armazenados os arquivos de responsabilidade de cada Setor Administrativo ou Coordenação, onde somente os membros de cada Setor ou Coordenação conseguem acessar e manipular os arquivos armazenados. • Esta pasta deve ser utilizada, preferencialmente, no armazenamento de arquivos que devem ser compartilhados entre os membros de cada Setor/Coordenação, mantendo-se o interesse institucional de seu armazenamento.
(X:) Pastas Públicas	• Arquivos de compartilhamento irrestrito e temporário. O conteúdo armazenado em pastas públicas não é garantido por nenhuma política de *backup* ou rotina de segurança periódica. • Esta pasta deve ser utilizada, preferencialmente, no armazenamento temporário de arquivos. • Esta pasta será periodicamente excluída pelo setor de suporte.
(W:) Pastas de Email	• Esta pasta mantêm os arquivos locais de armazenamento de *e-mails* do *Microsoft Outlook* 2003/2007. Esta pasta deve ser usada exclusivamente como recipiente do banco de dados de *e-mails* de cada usuário da SECONT.

	• Sua utilização é configurada automaticamente durante a instalação do *Microsoft Outlook* 2003/2007 nas estações de trabalho e *notebooks*.

7. Nas pastas PÚBLICAS devem ser armazenadas apenas informações comuns a todos os usuários. Estas não devem ser utilizadas para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível.
8. Haverá limpeza periódica das pastas PÚBLICAS, a critério do CSO em conjunto com o suporte de TI, para que não haja acúmulo desnecessário de arquivos.
9. É proibida a instalação ou a remoção de qualquer *software* sem o acompanhamento do Setor de Suporte Técnico. Quando necessário este serviço deverá ser solicitado via sistema interno de *Help Desk*.
10. O Setor de Suporte Técnico não fornecerá acessórios, software ou suporte técnico para computadores pessoais, incluindo assistência para recuperar perda de dados, decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software.
11. É obrigatório armazenar os arquivos de interesse da SECONT no servidor de arquivos, de forma a garantir a cópia de segurança dos mesmos.
12. É proibida a abertura de equipamentos para qualquer tipo de reparo, seja isto feito em departamentos ou laboratórios de informática e, quando necessário, o reparo ocorrerá sempre com o acompanhamento do Setor de Suporte Técnico.
13. Quando um usuário for transferido de setor, o coordenador/chefe de setor que o transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar a equipe de TI qualquer modificação

necessária. Esta informação deverá ser feita via sistema interno de Help Desk.

14. Quando ocorrer a exoneração do usuário, o coordenador/chefe responsável deve informar ao GRH e este deve solicitar, via sistema interno de Help Desk, que a equipe do Suporte Técnico providencie a desativação dos acessos do usuário a qualquer recurso da rede. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao setor.
15. Cada estação de trabalho/notebook possui códigos internos que permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho/notebook será de responsabilidade do usuário que a estiver utilizando. Por isso, sempre que sair da frente da estação de trabalho/notebook o usuário deve se certificar que efetuou o logoff ou a bloqueou.
16. Não é admitida a utilização de nenhum tipo de software/hardware desconhecido sem o conhecimento da equipe técnica.
17. Não é permitido gravar nas estações de trabalho/notebooks arquivos MP3, filmes, fotos e qualquer tipo de conteúdo que não tenha relação com as atividades da SECONT ou arquivos e softwares protegidos por direitos autorais sem o devido licenciamento.
18. Os arquivos gravados em quaisquer pastas dos discos locais das estações de trabalho e dos notebooks podem ser acessados por todos os usuários que utilizarem a mesma, portanto não se pode garantir sua integridade e disponibilidade. Poderão ser alterados ou excluídos sem prévio aviso e não farão parte das rotinas de segurança da SECONT.
19. Antes de mandar imprimir, o usuário deve verificar se a impressora está ligada, operacional e se não há nenhum trabalho de impressão de grande volume em andamento.
20. Se ocorrer erro na impressão e o papel puder ser reaproveitado na próxima tentativa, o usuário deve recolocá-lo na bandeja de impressão. Se o papel servir para rascunho, deverá levá-lo para sua mesa e, caso não tenha mais nenhuma utilidade, jogá-lo no lixo.

21. Não é permitido deixar impressões na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro de papel.
22. Se a impressora emitir alguma folha em branco, recoloque-a na bandeja.
23. Se o usuário notar que o papel de alguma das impressoras está no final, deverá fazer a gentileza de reabastecê-la. Isso evitará pedidos de impressão prejudicados e diminuirá o acúmulo de trabalho na fila de impressão.
24. A impressão colorida deverá ser utilizada somente para versão final de trabalhos e não para testes ou rascunhos. Toda impressão é monitorada, inclusive com geração de imagens do conteúdo impresso.
25. É proibida a impressão de qualquer conteúdo particular sem a devida autorização do chefe do setor ou do coordenador de área.

VI. NORMAS PARA CLASSIFICAÇÃO DE DOCUMENTOS ELETRÔNICOS

DO TRATAMENTO DE DOCUMENTOS SIGILOSOS

Os usuários da Rede Local da SECONT contam com recursos de *criptografia assimétrica* vinculados aos principais aplicativos de produção de documentos que devem ser utilizados, obrigatoriamente, em documentos classificados como secretos, internos ou confidenciais. No ato de criação destes documentos devem ser informados os usuários que terão acesso a eles e seus respectivos direitos de uso (acesso total, impressão, cópia, somente leitura, etc.).

Através da utilização correta destes recursos pode-se garantir a integridade e confidencialidade destes documentos, mesmo fora do ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT. Entretanto, este recurso não protegerá documentos físicos deixados expostos na mesa de trabalho, como por exemplo, relatórios, notas de auditoria ou outros documentos cujo conteúdo seja confidencial. Cabendo ao usuário, portanto, a responsabilidade pela guarda e pela proteção adequada deste tipo de documento.

SANÇÕES

De acordo com as diretrizes gerais desta política de segurança da informação, a SECONT se reserva o direito de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo a utilização de sua Rede Local.

A verificação do cumprimento das **Normas para Utilização da Rede Local** será efetuada da seguinte forma:

1. Os servidores do Setor de Suporte Técnico identificarão os usuários que violarem qualquer item da presente norma de segurança.
2. As transgressões das normas estabelecidas neste documento serão comunicadas ao transgressor, ao Secretário de Estado de Controle e Transparência e ao Coordenador/Chefe da área.
3. Caso a transgressão caracterize crime ou contravenção penal, será apresentada *notitia criminis* à Polícia Judiciária, sem prejuízo das sanções administrativas e cíveis cabíveis.

OBJETIVO

Estabelecer padrões, responsabilidades e requisitos básicos para a classificação dos documentos eletrônicos criados, manipulados e armazenados através do ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

ABRANGÊNCIA

Esta norma será aplicada a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação (TIC) da SECONT para criação, manipulação e armazenamentos de documentos eletrônicos.

CONCEITO

Documento eletrônico pode ser definido como um tipo de documento elaborado através de um computador e armazenado em dispositivo magnético e/ou óptico, sendo seu autor identificável por meio de um código, chave ou outro procedimento técnico.

Segundo **Camargo e Bellotto (Brasil - 1996)**, documento eletrônico é um tipo de documento cujo conteúdo, registrado em suportes especiais, é acessível apenas através de um computador.

O objetivo da classificação dos documentos eletrônicos é assegurar que estes ativos recebam um nível adequado de proteção. A informação neles armazenada pode possuir vários níveis de sensibilidade, além disso, alguns documentos podem necessitar de um nível adicional de proteção ou de tratamento especial.

Os usuários devem classificar os documentos eletrônicos produzidos ou custodiados pela SECONT de acordo com sua necessidade de confidencialidade, identificando-os como secreto, confidencial, interno ou público a partir da análise da sensibilidade das informações contidas no documento e das implicações de sua divulgação indevida.

O acesso e o uso dos documentos eletrônicos produzidos ou custodiados pela SECONT serão controlados de acordo com seus respectivos níveis de classificação.

Os documentos eletrônicos recebidos de pessoa física ou jurídica externa à SECONT serão submetidos às medidas de segurança da informação compatíveis com os requisitos pactuados com quem os forneceu.

Quando se tratar de informação sob a forma de sistema ou serviço de tecnologia da informação, a designação do proprietário ou custodiante, bem como a definição de suas responsabilidades ocorrerão mediante ato do Secretário de Estado de Controle e Transparência.

Classificação de Documentos Eletrônicos

A classificação dos documentos eletrônicos da SECONT será efetuada de acordo com o Decreto 3.152-R de 26 de novembro de 2012, que regulamenta a lei 9.871 que regula o acesso a informações previsto no inciso II do § 4º do artigo 32 da Constituição do Estado do Espírito Santo.

A Classificação dos documentos gerados pela SECONT será efetuada pela autoridade classificadora quando da análise de seu aspecto de divulgação ao público externo e se dividirá em quatro níveis: ULTRA-SECRETO, SECRETO, RESERVADO e PÚBLICO, este último por default independe de classificação.

A classificação interna dos documentos eletrônicos armazenados nos servidores da SECONT obedecerá a critérios próprios e se dividirá em 4 (quatro) níveis: Confidencial, Restrita, Uso Interno e Pública, conforme a seguir demonstrado.

Classificação	Descrição
Confidencial	As informações contidas em documentos classificadas como confidencial devem ser acessadas por um número restrito de pessoas e o controle sobre seu uso deverá ser total. Não são informações essenciais para a execução das atividades diárias da SECONT, porém, tem importância estratégica para o órgão e para o Governo como um todo. O acesso interno ou externo por pessoas não autorizadas e a posterior divulgação das informações armazenadas poderiam causar diversos prejuízos institucionais.
Restrita	Os documentos e informações classificados como restritos devem permanecer no ambiente interno da SECONT. O acesso a estes documentos deve ser feito de acordo com necessidades previamente estabelecidas, ou seja, os usuários somente poderão acessá-los se este acesso for fundamental para o desempenho satisfatório de suas funções no órgão. O acesso não autorizado a estes documentos eletrônicos poderia causar danos institucionais diversos.
Uso Interno	Os documentos eletrônicos classificados como internos não devem sair do âmbito da SECONT devendo ser armazenados em áreas próprias de cada grupo, setor ou coordenação ;
Pública	Os documentos eletrônicos classificados como públicos contêm informações que podem ser divulgadas para o público em geral, incluindo outros órgãos públicos, fornecedores e imprensa. Não possuem restrições para divulgação.

O ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT conta com recursos de proteção aos documentos eletrônicos através da aplicação de chaves de criptografia e da indicação de permissões de acesso persistentes, ou seja, as permissões de acesso são incorporadas aos documentos permitindo o acesso controlado dentro e fora do ambiente tecnológico do órgão.

As normas para classificação dos documentos eletrônicos são assim estabelecidas:

1. Todo e qualquer documento eletrônico produzido ou recebido através do ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT são em princípio classificados internamente como RESTRITOS e a sua divulgação ao público externo e a tramitação para outros órgãos passará pelo crivo do chefe imediato que identificará a necessidade ou não de classificação segundo o Decreto 3.152-R/2002;

2. O usuário responsável pela criação do documento eletrônico deverá armazená-lo na área própria destinada ao setor ao qual pertence, sendo vedado a sua distribuição a qualquer órgão público ou pessoa externa sem o conhecimento de seu superior hierárquico.

3. Após a classificação do documento eletrônico realizada no passo anterior, o usuário deverá efetuar as ações de proteção de acordo com o estipulado abaixo:

4. O criador de qualquer documento eletrônico no ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT será considerado "*proprietário*" do documento criado e "*custodiante*" das informações que ele armazena.

5. O proprietário de cada documento eletrônico da SECONT é pessoalmente responsável pelas informações mantidas no documento e pela aplicação das ações de segurança correspondentes ao nível de confidencialidade necessária ao documento.

6. A desclassificação do documento, que consiste em torná-lo público, é atribuição do Secretário de Estado de Controle e Transparência ou da autoridade competente para classificação delegada pelo Secretário.

7. Caso a divulgação das informações mantidas por um documento eletrônico que não tenha sido classificado, que tenha sido classificado de forma errônea ou cujas ações de segurança não foram adequadamente aplicadas acarrete danos institucionais ou financeiros para a SECONT, o proprietário do documento poderá ser responsabilizado solidariamente com o autor da divulgação.
8. A SECONT possui mecanismos de autenticação que determinam a titularidade da criação, do acesso e da manipulação de todos os documentos eletrônicos mantidos por sua infraestrutura de Tecnologia da Informação e Comunicação.
9. Haverá periodicamente a geração de relatórios gerenciais informando a titularidade dos documentos eletrônicos criados pelos usuários em determinado período. A direção do órgão poderá ter acesso a essas informações a qualquer tempo.
10. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso (nome de usuário e senha).
11. Será de responsabilidade de cada usuário zelar pelo fiel cumprimento do estabelecido pela presente norma.
12. A não observância de qualquer item acima resultará na aplicação das sanções previstas nas Diretrizes Gerais da Política de Segurança da Informação da SECONT.

VII. NORMAS PARA GESTÃO DE ATIVOS

OBJETIVO

Alcançar e manter a proteção adequada aos ativos do ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT, definindo as responsabilidades dos *proprietários*, *custodiantes* e *comodatários* de cada ativo tecnológico.

ABRANGÊNCIA

Esta norma aplica-se a todos os usuários que sejam proprietários, custodiantes ou comodatários dos ativos tecnológicos da SECONT. Esta norma também se aplica a qualquer usuário que de alguma forma interaja com esses ativos.

CONCEITOS

Segundo a norma ABNT NBR ISO/IEC 27001:2006, item 7.1, convém que todos os ativos sejam inventariados e tenham um proprietário responsável. Convém ainda que os proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles.

A implantação de controles específicos pode ser delegada pelo proprietário, porém o proprietário permanece responsável pela proteção adequada dos ativos.

Destarte, a SECONT elaborou esta norma de gestão de ativos, de forma a definir claramente quais as responsabilidades dos usuários designados como proprietário e/ou custodiante de algum ativo.

RESPONSABILIDADES: ATIVOS DO TIPO SERVIDOR

Do Proprietário

Todo ativo tecnológico do tipo servidor, instalado no *Datacenter* da SECONT terá designado um proprietário, que será responsável por:

1. Manter atualizadas as informações cadastrais sobre o ativo – *hardware*, *software* e serviços disponibilizados através daquele ativo.
2. Atuar como suporte nível três, conforme descrito neste documento.
3. Delegar para um custodiante, mediante acordo prévio, as tarefas de administração diária daquele ativo.
4. Coordenar as ações em casos de comprometimento da segurança lógica do ativo – invasões de *hackers*, pichação de *sites*, problemas na aplicação, etc.

5. Coordenar as ações necessárias para os casos de comprometimento da segurança física do ativo – danos, furto, roubo ou qualquer ameaça ambiental.

Observação: Dependendo da natureza do incidente, como, por exemplo, roubo ou furto de equipamento, a SECONT possui áreas exclusivas para tratar destes assuntos (Grupo Administrativo). Porém, é de inteira responsabilidade do proprietário do ativo interagir com essas áreas a fim de garantir que todas as providências necessárias sejam tomadas.

6. Manter atualizados todos os *softwares* que rodem naquele ativo, desde *upgrade* de versão à aplicação de *patches* de correção.

   Observação: Como um mesmo ativo pode ter várias aplicações pertencentes a diversas áreas dentro da SECONT (Exemplo: Banco de Dados, Sistema Operacional, Aplicações *WEB*), as atualizações de *software* deverão ser feitas diretamente por essas áreas, com intermédio do Setor de Suporte Técnico. Porém, cabe ao proprietário do ativo garantir que essas atualizações estão sendo realizadas e, em caso de não cumprimento deste item, notificar por escrito à Coordenação de Tecnologia da Informação dos problemas encontrados.

7. Ter chave de acesso com privilégio de leitura somente.

   Observação: O proprietário do ativo poderá ter acesso com privilégios de administrador sempre que precisar. Para tal, é necessário solicitar formalmente ao custodiante que conceda este acesso, informando sempre o período desejado e as tarefas que serão executadas, caso seja um servidor em produção.

8. Realizar estudos de planejamento de capacidade de forma a evitar sobrecarga nos sistemas suportados pelo ativo.

9. Definir e instalar novas funcionalidades. Exemplo: *upgrade* de versão, configuração de um novo serviço, etc.

10. Garantir que o sistema operacional e os aplicativos estejam sujeitos a um rígido controle de gestão de mudanças.
11. Os seguintes aspectos devem ser considerados quando um ativo for sofrer modificações:
    a. Identificação e registro das mudanças significativas.
    b. Planejamento e testes das mudanças.
    c. Avaliações de impactos potenciais, incluindo impactos de segurança.
    d. Procedimento formal de aprovação das mudanças propostas.
    e. Comunicação dos detalhes das mudanças para todas as pessoas envolvidas.
    f. Procedimentos de recuperação.
12. Criar e implantar os procedimentos para a geração de cópias de segurança – *Backup* – e sua recuperação – *Restore* – em um tempo aceitável.
13. Garantir que os registros (*log*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo determinado, para auxiliar em futuras investigações e monitoramento de controle de acesso.

Do Custodiante

Todo ativo tecnológico, do tipo servidor, instalado no *Datacenter* da SECONT terá designado um custodiante, que será responsável por:

1. Ajudar o proprietário a manter atualizadas as informações cadastrais sobre o ativo – *hardware*, *software* e os serviços disponibilizados através daquele ativo.
2. Atuar como suporte nível dois, conforme definido neste documento.

3. Cuidar do ativo no dia-a-dia, notificando ao proprietário qualquer anomalia encontrada.
4. Comunicar imediatamente ao proprietário qualquer problema de segurança do ativo – invasões de *hackers*, pichação de *sites*, problemas na aplicação, entre outros e as ações que foram tomadas para sanar ou minimizar o problema.
5. Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua custódia.
6. Atualizar, a pedido do proprietário, os *softwares* de qualquer natureza que funcionem no ativo, desde *upgrade* de versão à aplicação de *patches*.

   Observação: Toda a documentação necessária para realizar as atualizações deverá ter sido previamente fornecida pelo proprietário.
7. Ter chave de acesso com privilégio de administrador nos ativos sob sua custódia.
8. Realizar as modificações necessárias nos ativos, de acordo com o planejamento da gestão de mudanças definida pelo proprietário.
9. Garantir que as cópias de segurança – *backup* – estejam sendo geradas.
10. Monitorar os registros (*log*) de auditoria, avisando imediatamente ao proprietário qualquer problema encontrado.
11. Evitar o acesso aos ativos por pessoas não autorizadas.
12. Coibir qualquer modificação nos equipamentos ou no *software*, por quem quer que seja, exceto quando autorizada, por escrito, pelo proprietário do ativo.

Do Suporte

Ficam definidos três níveis de suporte para os ativos tecnológicos instalados no ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT, a saber:

Nível de Suporte	Responsável	Atividades
Suporte 1º Nível	Suporte Técnico.	Atendimentos iniciais com vista a manter a operacionalidade dos ativos e sistemas. Testes de conectividade, por exemplo: *ping*, *traceroute* e similares. Monitoramento de serviços. Aviso ao custodiante ou proprietário em caso de falhas ou mau funcionamento do ativo.
Suporte 2º Nível	Custodiante do ativo.	Realizar todas as atividades definidas para o custodiante. Quando na impossibilidade de resolução do problema, notificar o suporte de 3º nível.
Suporte 3º Nível	Proprietário do ativo.	Realizar todas as atividades definidas para o proprietário. Quando na impossibilidade de resolução do problema, acionar suporte externo.

RESPONSABILIDADES: ATIVOS DO TIPO ESTAÇÃO DE TRABALHO E *NOTEBOOK*

Do Proprietário e do Custodiante

O setor de Suporte Técnico da SECONT será designado proprietário e custodiante de todos os ativos tecnológicos do tipo Estação de Trabalho e *Notebook* e possuirá as seguintes atribuições:

1. Manter as informações cadastrais sobre os ativos atualizadas – *hardware*, *software* e serviços disponibilizados através daquele ativo.
2. Atuar como suporte nível três, conforme descrito neste documento.

3. Coordenar as ações necessárias para os casos de comprometimento da segurança do ativo – quebra de senha, problemas na aplicação, etc.
4. Manter atualizados todos os *softwares* que executem naquele ativo, desde *upgrade* de versão à aplicação de *patches* de correção.
5. Ter chave de acesso com privilégio total.
6. Realizar estudos de planejamento de capacidade de forma a evitar sobrecarga nos sistemas suportados pelo ativo.
7. Definir e instalar novas funções e funcionalidades. Exemplo: *upgrade* de versão, configuração de novo serviço, etc.
8. Garantir que o sistema operacional e os aplicativos estejam sujeitos a um rígido controle de gestão de mudanças.
9. Os seguintes aspectos devem ser considerados quando um ativo for sofrer modificação:
    a. Identificação e registro das mudanças significativas.
    b. Planejamento e testes das mudanças.
    c. Avaliações de impactos potenciais, incluindo impactos de segurança.
    d. Procedimento formal de aprovação das mudanças propostas.
    e. Comunicação dos detalhes das mudanças para todas as pessoas envolvidas.
    f. Procedimentos de recuperação.
10. Criar e implantar os procedimentos para a geração de cópias de segurança – *Backup* – e sua recuperação – *Restore* – em um tempo aceitável.
11. Garantir que registros (*log*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo determinado para auxiliar em futuras investigações e monitoramento de controle de acesso.

Do Comodatário

Será formalmente designado um comodatário para cada ativo tecnológico do tipo Estação de Trabalho e *Notebook* da SECONT e o mesmo possuirá as seguintes atribuições:

1. Coordenar as ações para os casos de comprometimento da segurança física do ativo – danos, furto, roubo ou qualquer ameaça ambiental.

   Observação: Dependendo da natureza do incidente, como, por exemplo, roubo ou furto de equipamento, a SECONT possui áreas exclusivas para tratar destes assuntos (Grupo Administrativo). Porém, é de inteira responsabilidade do comodatário do ativo interagir com essas áreas a fim de garantir que todas as providências necessárias sejam tomadas.

2. Ajudar o proprietário a manter atualizadas as informações cadastrais sobre o ativo – *hardware*, *software* e serviços disponibilizados através daquele ativo.

3. Cuidar do ativo no dia-a-dia, notificando ao proprietário qualquer anomalia encontrada.

4. Comunicar imediatamente ao proprietário qualquer problema de segurança lógica do ativo – quebra de senha, problemas na aplicação, etc.

5. Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua responsabilidade.

6. Atualizar, a pedido do proprietário, os *softwares* de qualquer natureza que rodem no ativo, desde *upgrade* de versão à aplicação de *patches*.

   Observação: Toda a documentação e permissão necessária para realizar as atualizações deverão ter sido previamente fornecidas pelo proprietário.

7. Ter chave de acesso com privilégio restrito nos ativos sob sua responsabilidade.

8. Evitar o acesso aos ativos por pessoas não autorizadas.

9. Coibir qualquer modificação nos equipamentos ou *softwares*, por quem quer que seja, exceto quando autorizada por escrito pelo proprietário do ativo;

10. O comodatário deverá utilizar, obrigatoriamente, o dispositivo "***hard lock***" que permite prender os ativos do tipo *Notebook* ao local de utilização.

RESPONSABILIDADES: DEMAIS ATIVOS TECNOLÓGICOS

Do Proprietário e do Custodiante

O setor de Suporte Técnico será designado como proprietário e custodiante de todos os demais ativos tecnológicos da SECONT (*roteadores*, *switches*, impressoras, etc.), devendo assumir as seguintes responsabilidades:

1. Manter as informações cadastrais sobre os ativos atualizadas – *hardware*, *software* e serviços disponibilizados através daquele ativo.
2. Coordenar as ações para os casos de comprometimento da segurança dos ativos – quebra de senha, problemas na aplicação, etc.
3. Coordenar as ações para os casos de comprometimento da segurança física do ativo – danos, furto, roubo ou ameaças ambientais.
4. Manter atualizados todos os *softwares/firmwares* que executem naquele ativo, desde *upgrade* de versão à aplicação de *patches* de correção.
5. Realizar estudos de planejamento de capacidade de forma a evitar sobrecarga nos sistemas suportados pelo ativo.
6. Definir e instalar novas funcionalidades. Exemplo: *upgrade* de versão, configuração de um novo serviço, etc.
7. Os seguintes aspectos devem ser considerados quando um ativo for sofrer modificações:
    a. Identificação e registro das mudanças significativas.
    b. Planejamento e testes das mudanças.
    c. Avaliações de impactos potenciais, incluindo impactos de segurança.

d. Procedimento formal de aprovação das mudanças propostas.

e. Comunicação dos detalhes das mudanças para todas as pessoas envolvidas.

f. Procedimentos de recuperação.

8. Garantir que registros (*log*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo determinado para auxiliar em futuras investigações e monitoramento de controle de acesso.
9. Cuidar do ativo no dia-a-dia.
10. Ter chave de acesso com privilégio de administrador nos ativos.

VIII. NORMAS PARA UTILIZAÇÃO DE CONTA E SENHA DOS USUÁRIOS

OBJETIVO

Estabelecer os procedimentos adequados para a correta utilização das contas e senhas dos usuários do ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

ABRANGÊNCIA

Esta norma se aplica a todos os usuários que possuam contas (sem privilégios administrativos) nos ativos do tipo estações de trabalho, *notebooks* e servidores do ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

CONCEITO

Segundo a norma ABNT NBR ISO/IEC 27001:2006, item 11.2, convém que procedimentos formais sejam utilizados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços. Convém ainda que a concessão e o uso de privilégios sejam restritos e controlados (item 11.2.2).

Destarte, a SECONT elaborou a presente norma para evitar o uso inapropriado de senhas, que pode vir a ser um grande fator de contribuição para falhas ou violações dos ativos tecnológicos.

FORMAÇÃO DE CONTAS E SENHAS

As senhas para usuários finais deverão conter no mínimo seis caracteres, obrigatoriamente, formadas por uma combinação de letras, números e caracteres especiais.

Os sistemas e aplicações devem prover algum mecanismo ou instrução que garanta que só sejam aceitas senhas com a formação acima citada. As contas, tanto de rede quanto de *e-mail*, serão criadas com o seguinte padrão: "*primeiro nome.último sobrenome*".

Deverá ser evitada a composição de senhas com sequências numéricas (123...) ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento, etc.).

Distribuição de Contas e Senhas

O Grupo de Recursos Humanos - GRH é responsável pelas solicitações de abertura das contas de rede e da criação dos *e-mails* vinculados a SECONT. Esta solicitação deve ser realizada através do sistema de *Help Desk* interno, indicando, no mínimo, as seguintes informações:

- Nome completo do usuário.
- Número funcional.
- Setor que o usuário será lotado.
- Nível de acesso a Internet (liberado ou restrito).
- Telefone do setor.

As contas de *e-mail* e de rede serão criadas com uma senha padrão que será informada pelo Suporte Técnico após o atendimento da solicitação de criação feita pelo GRH. Caberá ao usuário a imediata substituição da senha padrão informada, respeitando-se os critérios definidos na presente norma.

Tempo de Vida de Contas e Senhas

1. O usuário será forçado a trocar a senha no seu primeiro acesso. Será guardado um histórico composto de, pelo menos, seis das últimas senhas. As senhas guardadas no histórico não poderão ser utilizadas como novas senhas.
2. O tempo mínimo, por vontade do usuário, para troca de senhas deverá ser de dois dias.
3. A conta será bloqueada após a 5ª (quinta) tentativa de acesso.

4. O tempo de vida das senhas será de, no máximo, 45 (quarenta e cinco) dias, quando deverá ser forçada a sua troca no primeiro acesso após esse período.
5. Contas que ficarem inativas por mais de 90 (noventa) dias serão bloqueadas.

Reinicialização de Senhas

1. As contas somente poderão ser reinicializadas por solicitação formal do seu proprietário à área responsável pela administração das contas (Suporte Técnico).
2. A reinicialização de uma senha em sistemas críticos só ocorrerá em casos de extrema necessidade e mediante a confirmação de algumas informações de caráter pessoal do usuário. Nestes casos, o atendente/técnico deverá retornar a ligação para confirmação desses dados.
3. Para casos considerados críticos, a solicitação de reinicialização da conta deverá ser feita através de contato com o Coordenador de Auditoria ou com o Chefe do Setor.
4. Caso o usuário suspeite do comprometimento de sua senha, esta deverá ser modificada imediatamente.

Disposições Gerais

1. Os sistemas e aplicações terão mecanismos que impedirão a mesma conta de estar ativa, simultaneamente, em mais de uma estação de trabalho ou *notebook*.
2. Os sistemas e aplicações terão mecanismos que impedirão a exibição automática, na tela de entrada, da senha referente à respectiva conta em uso.
3. A senha é pessoal e intransferível, devendo ser mantida em sigilo. O usuário será responsabilizado pelo mau uso da mesma, conforme previsto na presente Política de Segurança da Informação.

4. O Grupo de Recursos Humanos deverá comunicar ao Suporte Técnico o desligamento ou remanejamento de qualquer servidor da SECONT. Esta comunicação deverá ser realizada pelo sistema de *Help Desk* interno.
5. Será atribuído o menor privilégio possível as contas dos usuários, que permitirá apenas a realização das tarefas pertinentes as suas atividades.
6. Os usuários finais não poderão ter contas com perfil de administrador, nem contas do domínio com privilégio de administrador local da estação.
7. Os sucessos e as falhas nas tentativas de acesso (*logon*) serão auditados.
8. A eventual necessidade de instalação de *software* deve ser solicitada via sistema interno de *Help Desk*, ao Setor de Suporte Técnico, de forma que possibilite um controle centralizado de *softwares* e licenças disponíveis para a SECONT.
9. No caso de necessidade de utilização temporária de equipamento de pessoal externo na Rede Local da SECONT, o mesmo deve ser submetido ao Setor de Suporte Técnico para que seja feita a configuração do equipamento como se fosse uma estação normal de trabalho do órgão, configurando a senha de administrador do Suporte Técnico, retirando outras contas com perfil administrativo e instalação de antivírus. O equipamento também deverá ser submetido à análise completa para a remoção de possíveis *softwares* maliciosos (*spywares*, *trojans*, etc.).

IX. NORMAS PARA UTILIZAÇÃO DE CONTA E SENHA DOS ADMINISTRADORES

OBJETIVO

Estabelecer os procedimentos adequados para a correta utilização das contas com privilégios de "administrador" das estações de trabalho, *notebooks* e servidores do ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

ABRANGÊNCIA

Esta norma se aplica a todos os usuários que possuam contas com privilégio de "administrador" nos ativos do tipo estações de trabalho, *notebooks* e servidores do ambiente de TI da SECONT.

CONCEITO

Segundo a norma ABNT NBR ISO/IEC 27001:2006, item 11.2, convém que procedimentos formais sejam implantados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços. Convém ainda que a concessão e o uso de privilégios sejam restritos e controlados (item 11.2.2).

A SECONT elaborou a presente norma para evitar o uso inapropriado de privilégios de administrador de sistemas, que pode vir a ser um fator de contribuição para falhas ou violações de ativos tecnológicos.

USUÁRIOS COM PRIVILÉGIOS DE ADMINISTRADOR

Os ativos do tipo estação de trabalho e *notebooks*, de propriedade da SECONT, instalados no próprio órgão ou em qualquer outro órgão do Estado, terão as seguintes regras para as senhas com privilégios de administrador:

1. Somente o proprietário deste ativo poderá ter contas com privilégios de administrador local.
2. Caso o custodiante deste ativo necessite, por motivos de trabalho, ter privilégios de administrador local na estação de trabalho ou *notebook* sob

sua custódia, o mesmo deverá solicitar ao seu superior imediato que envie um pedido formal (via *e-mail* ou Correspondência Interna - CI) à Coordenação de Tecnologia da Informação justificando seu pedido. O pleito será analisado e a autorização poderá ser concedida em casos específicos.

Os ativos do tipo servidor, instalados no Datacenter da SECONT, terão as seguintes regras para as senhas com privilégios de administrador:

1. O custodiante deste ativo terá a senha com privilégios de administrador.
2. O proprietário deste ativo terá senha com privilégios de leitura, total e irrestrito ao Sistema Operacional e nas aplicações que este servidor suportar (Exemplo: Banco de Dados, Serviços Internet, etc.).
3. O proprietário do ativo terá acesso com privilégios de administrador sempre que precisar. Para tal, é necessário solicitar formalmente ao custodiante que conceda este acesso, informando sempre o período desejado e as tarefas que serão executadas, caso seja um servidor em produção.
4. Todos os usuários que manipulam os ativos do tipo servidor, sejam como custodiantes ou proprietários, terão acesso a um inventário destes ativos, que estará disponível em meio magnético e conterá informações atualizadas sobre os responsáveis por cada servidor.

FORMAÇÃO DE CONTAS E SENHAS

1. As senhas para administradores deverão ser fortes e conter no mínimo 10 caracteres, sendo obrigatório o uso de letras maiúsculas, minúsculas e caracteres numéricos e especiais (“$”, “%”, “&”,...). Para aqueles ambientes que não suportarem o mínimo de 10 caracteres, deverão ser utilizados o limite que o ambiente permitir.
2. Os sistemas e aplicações deverão prover algum mecanismo ou instrução que garanta que só sejam aceitas senhas com a formação acima citada.

3. As contas com privilégio de administrador não poderão conter em sua formação algo que as identifique como sendo uma conta de administrador. (Exemplo: admin, adm, administrador, administrator, pradmin, etc.).
4. Deverá ser criada uma ou mais contas, sem nenhum privilégio, com formação que possa identificá-la como sendo uma conta de administrador. Essas contas serão constantemente submetidas à auditoria, com o propósito de verificar as tentativas de utilização das mesmas.
5. Deverão ser evitadas as composições de senhas com sequências numéricas (123...) e/ou alfabéticas (abc...).

TEMPO DE VIDA DE CONTAS E SENHAS

1. Deverá ser guardado um histórico composto, pelo menos, das 8 (oito) últimas senhas.
2. A conta deverá ser bloqueada após a 5ª (quinta) tentativa de uso.
3. O tempo de vida das senhas obedecerá aos seguintes critérios:
    a. Administrador de servidores e de domínio – validade de, no máximo, 90 (noventa) dias, devendo ser forçada a troca no primeiro *login* após esse período.
    b. Administrador local – válida por tempo indeterminado.

REINICIALIZAÇÃO DE SENHAS

1. Em caso de necessidade de utilização da senha do Administrador, a mesma deverá ser reinicializada após o uso, segundo os procedimentos descritos nas Disposições Gerais da presente norma.
2. Caso haja suspeita do comprometimento de uma senha, esta deverá ser reinicializada.

DISPOSIÇÕES GERAIS

1. Os sistemas e aplicações deverão ter mecanismo que impeça a mesma conta de estar ativa, simultaneamente, em mais de uma estação de trabalho ou *notebook*.
2. Os sistemas e aplicações deverão ter algum mecanismo que impeça a exibição automática, na tela de *login*, da senha referente ao respectivo *login* em uso.
3. A senha deverá ser mantida em sigilo pelo administrador durante o período de uso. O administrador será responsabilizado, conforme previsto na presente Política de Segurança da Informação, pelo mau uso da mesma.
4. Em caso de desligamento ou remanejamento de usuários, as áreas responsáveis pela administração das contas deverão realizar a troca das senhas de administrador, tanto para ativos do tipo estação de trabalho, *notebook* ou servidor.
5. Os ativos do tipo servidor, estação de trabalho ou *notebook* deverão ter, no máximo, duas contas com privilégio de administrador.
6. Os acessos realizados e as falhas nas tentativas de logon deverão ser auditados.

X. NORMAS PARA UTILIZAÇÃO DO SISTEMA DE MENSAGENS INTERNAS

OBJETIVO

Estabelecer responsabilidades e requisitos básicos para utilização do Sistema de Mensagens Internas no ambiente de Tecnologia da Informação e Comunicação (TIC) da SECONT.

ABRANGÊNCIA

Esta norma se aplica a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação da SECONT para acesso ao Sistema de Mensagens Internas.

CONCEITO

O Sistema de Mensagens Internas é uma facilidade oferecida pelo setor de Suporte Técnico da SECONT que permite uma troca rápida de mensagens de texto entre os usuários de sua Rede Local.

Sob o aspecto de proteção e integridade dos sistemas de informação, este sistema é classificado como conexão de baixo risco. Os usuários devem estar cientes, entretanto, que sua utilização deve ser regida por boas práticas e cuidados no envio e recebimento das mensagens.

Todos os usuários dos ativos de informação de propriedade ou custodiados pela SECONT, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

UTILIZAÇÃO DO SISTEMA DE MENSAGENS INTERNAS

As normas para utilização do sistema de mensagens internas são assim definidas:

1. A SECONT possui mecanismos de autenticação que determinam a titularidade de todas as mensagens enviadas pelos usuários.

2. É expressamente proibida a divulgação ou o compartilhamento de informações institucionais sigilosas no sistema de mensagens internas.
3. O usuário deve utilizar o sistema de mensagens internas de forma adequada e diligente.
4. O usuário deve utilizar o sistema de mensagens internas observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública.
5. O usuário deve abster-se de utilizar o sistema de mensagens internas com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente norma, lesivos aos direitos e interesses do órgão ou de terceiros.
6. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso (nome de usuário e senha) no sistema de mensagens internas.
7. Será de responsabilidade de cada usuário zelar pelo cumprimento do estabelecido nesta norma.
8. A não observância de qualquer item acima implicará nas sanções previstas nas Diretrizes Gerais da Política de Segurança da Informação da SECONT.

SANÇÕES

De acordo com as diretrizes gerais desta política de segurança da informação, a SECONT se reserva o direito de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo o envio e recebimento de mensagens instantâneas.

A verificação do cumprimento das **Normas para Utilização do Sistema de Mensagens Internas** será efetuada da seguinte forma:

1. Os servidores do Setor de Suporte Técnico identificarão os usuários - doravante chamados de infratores - que violarem qualquer item da presente norma de segurança.
2. As transgressões das normas estabelecidas neste documento serão comunicadas ao transgressor, ao Secretário de Estado de Controle e Transparência e ao Coordenador/Chefe da área.

3. Caso a transgressão caracterize crime ou contravenção penal, será apresentada *notitia criminis* à Polícia Judiciária, sem prejuízo das sanções administrativas e cíveis cabíveis.

XI. NORMAS GERAIS PARA MANUSEIO DE PROCESSOS OU QUAISQUER OUTROS DOCUMENTOS TRAMITADOS NA SECONT

OBJETIVO

Estabelecer responsabilidades e requisitos básicos para o zelo e trato de informações, processos ou quaisquer outros documentos com carga para a SECONT.

ABRANGÊNCIA

Esta norma se aplica a todos os usuários que manipulam processos, ofícios, memorandos, cartas ou quaisquer outros documentos produzidos ou encaminhados à SECONT.

CONCEITO

Os documentos físicos ou eletrônicos encaminhados à SECONT são de propriedade do órgão que os produziu, e são confiados à Secretaria em razão da natureza de suas atribuições.

Sob o aspecto de proteção e integridade, constitui alto risco o tramite externo não autorizado de documentos. Os usuários devem estar cientes, de que a perda de processos, ofícios ou quaisquer outros documentos físicos ou eletrônicos podem gerar transtornos com consequências irreparáveis.

MANUSEIO DE DOCUMENTOS E INFORMAÇÕES TRAMITADOS PELA SECONT

As normas para utilização do sistema de mensagens internas são assim definidas:

1. A SECONT possui mecanismos de autenticação que determinam a titularidade da manipulação de documentos eletrônicos (cópias, impressões, envio eletrônico entre outros).

2. É expressamente proibida a divulgação ou o compartilhamento de informações tramitadas para a SECONT ou por esta produzida, ainda que as mesmas não sejam classificadas como sigilosas.
3. É expressamente proibido a retirada de documento, processo ou qualquer outra correspondência física para manuseio particular fora do ambiente da SECONT.
4. Caso seja estritamente necessário, em razão de suas atividades e motivado pela necessidade do trabalho, o funcionário deverá providenciar cópia do documento ou processo, ficando o original restrito ao ambiente da SECONT.
5. O usuário é pessoalmente responsável pelo extravio, roubo ou furto de documentos de trabalho em sua posse.
6. A não observância de qualquer item acima implicará nas sanções previstas nas Diretrizes Gerais da Política de Segurança da Informação da SECONT.

SANÇÕES

De acordo com as diretrizes gerais desta política de segurança da informação, a SECONT se reserva o direito de monitorar o uso de sua rede de computadores.

A verificação do cumprimento desta Norma se dará conforme a seguir discriminado:

1. Os servidores do Setor de Suporte Técnico identificarão, sempre que possível, os usuários que violarem qualquer item da presente norma de segurança.
2. As transgressões das normas estabelecidas neste documento serão comunicadas ao transgressor, ao Secretário de Estado de Controle e Transparência e ao Coordenador/Chefe da área.
3. Caso a transgressão caracterize crime ou contravenção penal, será apresentada *notitia criminis* à Polícia Judiciária, sem prejuízo das sanções administrativas e cíveis cabíveis.

XII. MODELO DO TERMO INDIVIDUAL DE RESPONSABILIDADE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Termo Individual de Responsabilidade

Pelo presente instrumento, eu, _____, número funcional _____, na qualidade de usuário dos recursos de processamento de informação da SECONT, declaro estar ciente e concordar com a Política de Segurança da Informação composta por suas Diretrizes Gerais e Normas, que estão disponíveis em formato eletrônico no servidor \\serv003\Diversos\PSI.

Declaro estar ciente de que os acessos por mim realizados à internet, ao sistema de mensagens internas, bem como o conteúdo das mensagens enviadas através do correio eletrônico institucional são monitorados automaticamente.

Declaro, ainda, estar ciente das minhas responsabilidades descritas nas Normas da Política de Segurança da Informação e que a não observância desses preceitos implicará na aplicação das sanções previstas nas Diretrizes Gerais desta Política.

Declaro ter conhecimento de que os recursos de processamento de informação disponíveis pela SECONT somente podem ser utilizados por aqueles que assinaram o presente Termo de Responsabilidade.

Vitória/ES, __ de _____ de 20__.

(Assinatura)

XIII. MODELO DO TERMO INDIVIDUAL DE CONFIDENCIALIDADE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Termo Individual de Confidencialidade

Eu, _____, número funcional _____, comprometo-me a manter confidencialidade com relação a toda documentação e toda informação obtida através de minhas atividades na SECONT, ou através de qualquer pessoa física ou jurídica vinculada de alguma forma à SECONT, concordando em:

1. Não divulgar a terceiros a natureza e o conteúdo de qualquer informação que componha ou contenha resultado de atividades da SECONT;
2. Não permitir a terceiros o manuseio de qualquer documentação que componha ou contenha resultado de atividades da SECONT;
3. Não explorar, em benefício próprio, informações e documentos adquiridos através da participação em atividades da SECONT;
4. Não permitir o uso por outrem de informações e documentos adquiridos através da participação em atividades da SECONT;
5. Não copiar, ou distribuir informações de bancos de dados, ou qualquer outro meio custodiado pela SECONT a terceiros.

Declaro ter conhecimento de que as informações e os documentos pertinentes às atividades da SECONT somente podem ser acessados por aqueles que assinaram o presente Termo Individual de Confidencialidade, excetuando-se os casos em que a quebra de confidencialidade é inerente à atividade ou em que a informação ou documentação já for de domínio público.

Vitória/ES, __ de _____ de 20__.

(Assinatura)

XIV. GLOSSÁRIO

Administrador	Nome de uma conta de usuário que normalmente permite acesso total e irrestrito a quaisquer recursos do sistema em que estão vinculadas.
Arquivos infectados	São arquivos que sofreram a ação de vírus eletrônico ou qualquer outro tipo de código malicioso.
Ativo	Qualquer item físico ou lógico que tenha valor para a organização [ISO/IEC 13335-1:2004] ou ainda qualquer instrumento que manipule direta ou indiretamente uma informação.
Caixa postal	Espaço em disco onde são armazenadas as mensagens de correio eletrônico.
Chave de acesso	Código de acesso atribuído a cada usuário. A cada chave de acesso é associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-lhe o acesso aos recursos disponíveis.
Códigos maliciosos ou agressivos	Qualquer código desenvolvido com a intenção de causar dano ou modificar o funcionamento correto de um sistema, como, por exemplo, um vírus eletrônico.
Comodato	Tipo de contrato de empréstimo em que a própria coisa emprestada deve ser restituída, não podendo haver restituição de coisa do mesmo gênero, qualidade ou quantidade, como é o caso do empréstimo mútuo.
Conta	Idem chave de acesso.
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.
Criptografia Assimétrica	Tecnologia que torna qualquer dado (texto, arquivo, e-mail) ilegível mediante embaralhamento e substituição dos dados num padrão que só uma chave pública consegue fazer e só a chave privada correspondente consegue desfazer.
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].
Custodiar	Conservar em custódia; vigiar; guardar; proteger.
Download	Processo que permite receber arquivos armazenados em outros computadores, geralmente através da Internet.
Ferramenta tecnológica	No contexto da presente Política pode ser entendido como um sistema ou equipamento destinado a proteger, monitorar ou agregar valor aos ativos de informação.
FTP (File Transfer Protocol)	Protocolo usado para transferência de arquivos entre computadores.
IMAP (Internet Message Access Protocol)	Protocolo de acesso a mensagens eletrônicas.
Incidente de segurança	Qualquer indício de fraude, sabotagem, desvio, falha, evento indesejado ou inesperado que tenha probabilidade de comprometer as operações ou ameaçar a segurança de informações de propriedade ou custodiado pela SECONT.
Informações eletrônicas	São aquelas pertencentes a terceiros, sendo de responsabilidade dos órgãos públicos a sua guarda, utilização e divulgação controlada.

controladas pelo governo	
Informações eletrônicas de propriedade do governo	São aquelas geradas nos ambientes tecnológicos dos órgãos governamentais.
Internet	Associação mundial de redes de computadores 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.
Licença de software	Direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade intelectual.
Modem	Equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações.
Órgão público	Qualquer ente da Administração Pública Direta ou Indireta.
Peer-to-Peer (P2P)	É um tipo de conexão que permite a distribuição de arquivos a outros usuários através da Internet.
POP (Post Office Protocol)	Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.
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].
Servidor de correio eletrônico	Equipamento que provê o serviço de envio e recebimento de mensagens de correio eletrônico.
Sistemas informatizados	Sistema constituído de programas e equipamentos computacionais.
Site	Conjunto de páginas que podem conter imagens, fotos, textos, vídeos, sons, etc. Ficam armazenadas em servidores que, normalmente, podem ser acessados através da Internet.
Site de proxy	São sites que permitem acessar conteúdo bloqueado pela Política de Segurança através do redirecionamento das requisições de conexão.
SMTP (Simple Mail Transfer Protocol)	Protocolo de comunicação usado para envio de mensagens na Internet via correio eletrônico.
Software	Programa de computador.
Spam	Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado.
Upload	Envio de um arquivo de seu computador para outro, normalmente, através da Internet.
URL (Uniform Resource Locator)	Endereço de uma página WEB, como, por exemplo: http://www.secont.es.gov.br
Usuário colaborador	Prestador de serviço terceirizado, estagiário ou qualquer colaborador da SECONT que tenha acesso, de forma autorizada, as informações eletrônicas produzidas ou custodiadas pelo órgão.
Usuário externo	Qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, as informações eletrônicas produzidas

	ou custodiadas pela SECONT e que não seja caracterizada como usuário interno ou usuário colaborador.
Usuário interno	Qualquer servidor ativo que tenha acesso, de forma autorizada, aos sistemas e as informações produzidas eletronicamente ou custodiadas pela SECONT.
Usuários	Servidores, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários que utilizem os recursos do ambiente tecnológico da SECONT.
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.