ATO Nº 387, de 1º de setembro de 2010

Institui a Política de Segurança no âmbito da Tecnologia da Informação para o Tribunal de Contas do Estado da Bahia (TCE/BA), estabelece as suas normas de operacionalização e dá outras providências.

A Presidente do Tribunal de Contas do Estado da Bahia, no uso das atribuições estabelecidas no inciso I do artigo 6º, do Regimento Interno deste Tribunal e,

CONSIDERANDO que a informação é um dos principais ativos do TCE/BA e é recurso fundamental para a consecução da missão e dos objetivos estratégicos da Administração;

CONSIDERANDO que as normas da Associação Brasileira de Normas Técnicas NBR ISO/IEC 27001:2006 e 27002:2005 estabelecem as melhores práticas na área de segurança da informação;

CONSIDERANDO que a segurança da informação visa garantir a confidencialidade, a integridade e a disponibilidade das informações usadas pelo TCE/BA, independente do meio físico em que se encontrem;

CONSIDERANDO que a existência e disseminação de códigos maliciosos podem provocar sérios danos aos Ativos de Informação e recursos de tecnologia do TCE/BA;

CONSIDERANDO que a internet e o correio eletrônico são ambientes de risco elevado, requerendo medidas de proteção adequadas, tanto no aspecto técnico, quanto em termos de procedimentos de uso;

CONSIDERANDO que o advento de dispositivos móveis tornou possível o transporte de informações, além dos limites físicos do TCE/BA;

CONSIDERANDO que o art. 5.º, incisos X e XII, da Constituição Federal de 1988 estabelecem a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, e o sigilo da correspondência e das comunicações.

RESOLVE:

Instituir a Política de Segurança no âmbito da Tecnologia da Informação no TCE/BA, que será operacionalizada de acordo com as normas e disposições estabelecidas neste Ato.

I – DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO
Art. 1º – Fica criado o Comitê de Segurança da Informação, de caráter permanente, composto por 5 (cinco) membros designados por Ato da Presidência do Tribunal de Contas do Estado da Bahia.

Art. 2º – Compete ao Comitê de Segurança da Informação, dentre outras atribuições correlatas:

I. Manter sistemática de avaliação e monitoramento permanente dos processos de trabalho quanto aos riscos de segurança da informação;

II. Verificar o cumprimento das normas estabelecidas neste Ato;

III. Propor medidas operacionais de aperfeiçoamento para a gestão da segurança da informação, visando a prevenção de incidentes e a eliminação de fragilidades de segurança da informação;

IV. Propor, à Presidência do TCE/BA, alterações na presente Política de Segurança e nas suas normas de operacionalização;

V. Propor normas e medidas operacionais visando a gestão da contingência, com o objetivo de garantir a continuidade do negócio do TCE/BA;

VI. Propor ações destinadas à conscientização e à capacitação dos recursos humanos sobre a Política e as Normas de Segurança da Informação, bem como sobre as recomendações e boas práticas de segurança da informação.

II – DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 3º - A gestão da segurança da informação deve ser pautada pelas seguintes diretrizes:

I. Responsabilidade e comprometimento dos titulares das unidades técnicas e administrativas e dos seus servidores e colaboradores;

II. Padronização de processos de trabalho e soluções;

III. Otimização da alocação de recursos por meio da gestão de riscos de segurança da informação;

IV. Adoção consistente e racionalizada de tecnologias de segurança.

Art. 4º - É responsabilidade das unidades do TCE/BA e do CEDASC, no âmbito da sua competência:

I – Do CEDASC:
a) Gerir a segurança da informação de forma permanente;

b) Mapear e avaliar, periodicamente, os processos de trabalho quanto aos riscos de segurança da informação;

c) Inventariar, classificar e proteger adequadamente os ativos de informação;

d) Garantir que as condições físicas e ambientais das instalações estejam em conformidade com as normas de segurança da informação;

e) Estabelecer um processo de gestão para a prevenção de incidentes e a eliminação de fragilidades de segurança da informação;

f) Estabelecer medidas para a gestão da contingência visando garantir a continuidade do negócio do TCE/BA;

g) Estabelecer e divulgar as rotinas de realização de cópias de segurança de arquivos e sistemas corporativos;

h) Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos, de forma continuada, sobre a Política e as Normas de Segurança da Informação, bem como sobre as recomendações e boas práticas de segurança da informação;

i) Prestar informações periódicas ao Comitê de Segurança da Informação para viabilizar a execução das suas competências.

II – Das Unidades técnicas, administrativas e de assessoramento do TCE/BA, bem como Gabinetes de Conselheiros:

a) Cumprir a política de segurança e as suas normas de operacionalização;

b) Auxiliar o CEDASC na gestão da política de segurança;

c) Apresentar sugestões de aperfeiçoamento da Política de Segurança e das normas de operacionalização ao Comitê de Segurança da Informação.

III - NORMA DE CONTROLE DE ACESSO LÓGICO
E DE RESPONSABILIDADE DOS USUÁRIOS

Art. 5º - Todo usuário terá uma conta de acesso própria, responsabilizando-se por todos os eventos a ela relacionados.

§ 1.º - Será definido um padrão de conta de usuário para acesso aos recursos computacionais do TCE/BA.

§ 2.º - A conta de usuário deve ser única em todos os ambientes e sistemas, devendo ser a mesma usada para aplicações, e qualquer outro ambiente ao qual o usuário possua acesso.

§ 3.º - Uma conta de acesso somente será criada mediante requerimento formal do chefe da unidade onde o usuário desempenha suas atividades.

§ 4.º - Será estabelecido um processo de bloqueio automático da sessão, depois de transcorridos 15 (quinze) minutos de inatividade de ações do usuário.

§ 5.º – A conta de usuário sem atividade e que não tenha acessado os recursos computacionais do TCE/BA após 90 (noventa) dias será bloqueada das bases de dados de usuários ativos.

§ 6.º – A conta de usuário sem atividade e que não tenha acessado os recursos computacionais do TCE/BA após 180 (cento e oitenta) dias será eliminada das bases de dados de usuários ativos, podendo ser guardada em base histórica para futuras auditorias ou referências de acessos antigos.

§ 7.º - Não são permitidas contas de acesso para grupos de usuários, nem é permitido o uso de contas de acesso genéricas.

§ 8.º - Os eventos relacionados a uma determinada conta de usuário serão associados ao seu proprietário.

Art. 6º – A senha é pessoal e intransferível, sendo responsabilidade do usuário a sua proteção.

Parágrafo único: O usuário deve manter sigilo sobre sua senha e esta não deve ser compartilhada ou divulgada a terceiros.

Art. 7º - Compete ao CEDASC:

I - Conceder, alterar e/ou revogar a permissão de acesso e efetuar revisão periódica dos respectivos direitos, mediante autorização dos responsáveis pelo ativo da informação;

II - Operacionalizar as ferramentas de controle de acesso lógico, a fim de unificar as contas de cada usuário;

III – Implantar e manter ferramentas, a exemplo de firewall, sistemas de detecção de intrusos, etc, e procedimentos de prevenção para que usuários não autorizados, internos e externos, não se conectem ou acessem ativos da informação, monitorando e verificando, periodicamente, todos os acessos e direitos concedidos;

IV – Implementar mecanismos de proteção contra contaminação por códigos maliciosos nos equipamentos em uso pelo TCE/BA;

V – Monitorar, a pedido do Comitê de Segurança da Informação, o uso dos recursos de tecnologia da informação;

VI – Adotar e divulgar uma política e as boas práticas de criação e uso de senha para a autenticação de usuários para acesso aos sistemas.

Art. 8.º – Compete aos chefes de unidade informar o desligamento e/ou movimentação de usuários, tais como afastamentos, nomeações, exonerações e alterações de lotação, à Gerência de Recursos Humanos e ao CEDASC.

Parágrafo único: Adicionalmente, cabe à Gerência de Recursos Humanos comunicar formalmente as ocorrências ao CEDASC, quando do seu lançamento no respectivo sistema informatizado.

IV - NORMA DE USO DO CORREIO ELETRÔNICO

Art. 9º - O serviço de correio eletrônico do TCE/BA deve ser utilizado apenas para fins de interesse da Administração, sempre através do software homologado pelo CEDASC e pelo Comitê de Segurança da Informação.

Art. 10 - O serviço de correio eletrônico deve ser concedido exclusivamente àqueles usuários que necessitem deste serviço para suas atividades.

Art. 11 – Os usuários deverão ser titulares de uma única caixa postal individual no servidor de correio eletrônico.

Parágrafo único – Poderá ser criada, mediante justificativa fundamentada, caixa postal específica para uma unidade ou serviço, sempre vinculada, individualmente, ao servidor indicado na solicitação para a criação da caixa postal.

Art. 12 – O uso de correio eletrônico, para fins de interesse da Administração, será exclusivamente através de provedor do domínio tce.ba.gov.br.

Art. 13 - O uso de correio eletrônico, para fins pessoais, será exclusivamente através de webmail, sendo vedado o uso do domínio tce.ba.gov.br.

Parágrafo único: O conteúdo das mensagens poderá ser submetido a verificações de segurança, para proteger o ambiente de TI do TCE/BA, sem necessidade de prévia comunicação ao usuário, sendo assegurada a privacidade dos registros.

Art. 14 – É proibido o envio de mensagens de conteúdo impróprio, a exemplo daqueles relativos a pornografia, racismo, violência, incitação ao ódio, cyberbullying, discriminação religiosa, propaganda político-partidária, invasão de computadores, “correntes”, “pirâmides” e jogos de azar, com uso da estrutura de tecnologia da informação do TCE/BA, tanto hardwares, quanto softwares ou serviços.
Parágrafo único: O TCE/BA não se responsabiliza por mensagens de conteúdo impróprio, enviadas ou recebidas através de seu domínio tce.ba.gov.br.

Art. 15 - Não é permitido o envio de mensagem, através do correio eletrônico, sem a identificação do emissor.

Art. 16 – Presume-se que toda informação criada, armazenada e transmitida pelos computadores ou rede do TCE/BA, através do sistema de correio eletrônico corporativo, não é de caráter pessoal.

Art. 17 – O usuário deve informar ao CEDASC a ocorrência de qualquer incidente e potenciais ameaças à segurança da informação, inclusive mensagens de conteúdo impróprio.

V – NORMA DE USO DA INTERNET

Art. 18 - A permissão de acesso à internet deve ser concedida através de uma conta de usuário que possibilite identificar, individualmente, o usuário proprietário

Art. 19 - Não é permitido suprimir, omitir ou dissimular a identificação da conta de usuário a qualquer serviço da internet.

Art. 20 – É vedado o acesso ao ambiente de rede do TCE/BA, à internet ou a qualquer outra rede pública, através de mecanismo adicional de acesso simultâneo, a exemplo de modens ou rede de telefonia móvel, em conjunto com os serviços homologados pelo TCE/BA.

Art. 21 - Os usuários que desejarem utilizar outras conexões, além daquelas homologadas, deverão, obrigatoriamente, comunicar de maneira formal ao CEDASC, a fim de não comprometer a segurança da rede do TCE/BA.

Art. 22 – A comunicação entre computadores remotos e o ambiente interno do TCE/BA, através da internet ou de outra rede pública, deverá ser autenticada e criptografada, usando soluções tecnológicas homologadas pelo CEDASC.

Art. 23 – A comunicação entre o ambiente do TCE/BA e a internet ou qualquer outra rede pública deve, necessariamente, passar por firewalls, os quais serão configurados com política restritiva e permitir o monitoramento do fluxo de comunicação.

Art. 24 - O CEDASC pode, ad referendum do Comitê de Segurança da Informação, restringir ou bloquear o acesso a sítios, serviços da Internet ou download de arquivos, em caso de ameaça à segurança da informação ou por razões técnicas.

Art. 25 – O histórico de acessos poderá ser registrado, sem necessidade de prévia comunicação ao usuário, sendo assegurada a privacidade dos registros.
Art. 26 – É considerado como uso aceitável da internet:

I – acessar sítios de noticiários, contribuintes, órgãos públicos, fornecedores e quaisquer outras fontes de informação necessárias à execução das atividades dos usuários do TCE/BA;

II – utilizar serviços, para fins pessoais, prestados através da internet, tais como banco on-line, reserva de passagens, serviços de órgãos públicos, entre outros, de forma moderada e limitado ao estritamente necessário;

III – utilizar sistemas de correio web para fins pessoais, a exemplo de Yahoo, Hotmail, UOL, Gmail e etc., de forma moderada e limitado ao estritamente necessário.

Art. 27 – É vedado:

I - o acesso a sítios e serviços, inclusive de áudio e vídeo em tempo real, que o CEDASC ou o Comitê de Segurança da Informação identifiquem ameaça à segurança ou comprometimento do desempenho da rede do TCE/BA;

II - o acesso a sítios e serviços de conteúdos impróprios, assim considerados aqueles relativos a pornografia, racismo, violência, incitação ao ódio, invasão de computadores, jogos, entre outros, devendo o usuário sair imediatamente de qualquer sítio desta natureza assim que detectá-los;

III – o download, o armazenamento, a cópia, a exibição e a transmissão de arquivos protegidos por direitos autorais, tais como filmes, músicas, videoclipes, publicações e conteúdos semelhantes;

IV – a obtenção, o armazenamento ou a transmissão de conteúdo ilegal, tais como software não licenciado, senhas de terceiros, números de cartões de crédito de terceiros, entre outros;

V – a transferência de arquivos através de serviços de mensagem instantânea, tais como ICQ, MSN, Skype ou Messenger, seja por software específico ou via Web;

VI - o uso de aplicações ponto-a-ponto para distribuição de arquivos, tais como Kazaa, Napster, Emule, Torrent e correlatos;

VII - o uso ou a posse de ferramentas de hardware e software para sondagem, investigação ou teste de vulnerabilidade em computadores e sistemas, monitoramento de rede, comprometimento de sistemas, ataques e captura de dados;

VIII - o uso de jogos on-line.

Art. 28 - O download de arquivos permitidos, com grande volume de dados, deve considerar as limitações da conexão com a internet e, sempre que possível, deve ser executado fora do horário normal de expediente.

Art. 29 - Todo arquivo obtido em fontes externas ao TCE/BA e ao CEDASC deve ser submetido à verificação de software antivírus antes de ser utilizado.

VI - NORMA DE USO DE COMPUTAÇÃO MÓVEL E FIXA

Art. 30 - A utilização dos equipamentos ficará condicionada à prévia assinatura de Termo de Recebimento e Responsabilidade.

Parágrafo único – Os usuários deverão cumprir as normas, procedimentos e orientações quanto ao manuseio, à limpeza, à guarda, à proteção e ao transporte dos equipamentos.

Art. 31 – A posse e o uso dos equipamentos móveis está condicionada aos casos em que não seja viável o uso de equipamentos fixos.

Parágrafo único - Um usuário não poderá ser responsável, ao mesmo tempo, por microcomputadores móveis e fixos, salvo em casos excepcionais, nos quais os equipamentos móveis poderão ser disponibilizados para tarefa específica e por prazo determinado.

Art. 32 – É vedada a cessão ou transferência dos equipamentos móveis e fixos a terceiros, inclusive a outros servidores do TCE/BA.

Art. 33 – Os equipamentos móveis e fixos serão usados, exclusivamente, nos projetos e atividades do TCE/BA, vedado o uso para fins pessoais.

Art. 34 - Os equipamentos móveis devem ficar sob vigilância permanente do usuário responsável, inclusive nos casos de viagens.

Parágrafo único: É obrigatório o uso de trava de segurança, tanto nas dependências do TCE/BA, quanto fora delas.

Art. 35 – Somente poderão ser instalados nos microcomputadores móveis e fixos, softwares homologados pelo CEDASC, sendo vedada a instalação ou execução de softwares não autorizados.

Art. 36 – É vedado ao usuário utilizar de quaisquer mecanismos para impedir o pleno funcionamento dos softwares de segurança implementados pelo CEDASC.

Parágrafo único – O CEDASC realizará verificações periódicas automatizadas nos computadores fixos e portáteis, com o intuito de verificar uma possível contaminação no equipamento, promovendo sua imediata regularização, caso seja detectada qualquer anormalidade.
Art. 37 – O usuário deverá bloquear o acesso ao seu computador quando o mesmo estiver ligado e sem uso, em caso de breves ausências.

Art. 38 – É obrigação do usuário manter os equipamentos móveis e fixos em boas condições de funcionamento, bem como conservar as placas de tombo, sem removê-las.

Parágrafo único - O usuário é responsável pelos danos ou prejuízos que, em face de sua conduta, sejam causados aos equipamentos.

Art. 39 – As manutenções corretivas ou preventivas dos equipamentos móveis e fixos serão realizadas exclusivamente pelo CEDASC, ou por terceiro formalmente autorizado pelo CEDASC.

Art. 40 – Os usuários de equipamentos móveis e fixos devem fazer cópias periódicas dos dados armazenados nos computadores, a fim de assegurar que não haverá perda de informações, para os casos de danos físicos ou roubo do equipamento.

Art. 41 – Os usuários deverão utilizar o servidor de arquivos corporativo para armazenar as informações relacionadas às suas atividades no TCE/BA.

Parágrafo único – As informações armazenadas nos computadores móveis e fixos não serão objeto de cópias de segurança pelo CEDASC.

Art. 42 – É vedada a conexão à rede do TCE/BA de equipamentos particulares, tanto de usuários cadastrados, quanto de visitantes, salvo em situações excepcionais, mediante solicitação devidamente fundamentada do usuário, prévia autorização formal do CEDASC e cumprimento dos requisitos de segurança.

Art. 43 – Os usuários de equipamentos móveis deverão, a cada 12 (doze) meses de uso, apresentá-los ao CEDASC para verificação do cumprimento desta Norma.

Parágrafo único: O CEDASC poderá, a qualquer tempo, convocar os usuários para apresentar os equipamentos em prazo a ser estabelecido.

Art. 44 – Os usuários de equipamentos móveis deverão participar de treinamentos específicos para os quais sejam convocados pelas áreas competentes.

VII - NORMA DE TRABALHO REMOTO

Art. 45 – O trabalho remoto somente será permitido mediante o respeito às regras e diretrizes da Política de Segurança da Informação.

Art. 46 – O TCE/BA definirá, formalmente, quais usuários terão permissão para exercer atividades através de trabalho remoto, cabendo ao CEDASC o gerenciamento das permissões de acesso.
Art. 47 – O CEDASC manterá controle dos acessos, armazenando o histórico com a identificação do usuário, data, hora e recursos acessados.

Art. 48 - O usuário com autorização de acesso remoto utilizará o mesmo código de acesso e senha da rede do TCE/BA.
VIII – DISPOSIÇÕES FINAIS

Art. 49 – O CEDASC implementará as regras definidas nesta Norma, sendo responsável, também, pela adoção de medidas técnicas adicionais necessárias à manutenção da infraestrutura para acesso remoto e à otimização do uso dos recursos de tecnologia da informação.

Art. 50 - O CEDASC poderá, a qualquer tempo, verificar os computadores, com o objetivo de averiguar e identificar possíveis não-conformidades descritas nesta Norma.

Art. 51 – O CEDASC fará a divulgação de boas práticas quanto ao uso seguro da tecnologia da informação no âmbito do TCE/BA;

Art. 52 – Os usuários deverão conhecer e cumprir as orientações de segurança quanto ao uso correto e manuseio adequado dos recursos de tecnologia do TCE/BA.

Art. 53 – É de responsabilidade do usuário o respeito integral às leis de proteção à propriedade intelectual, sendo presumido que os direitos são reservados para todo conteúdo disponível na Internet, a menos que contenha informação explícita em contrário.

Art. 54 – É de responsabilidade do CEDASC comunicar ao TCE/BA a detecção de ocorrência de possível descumprimento, pelo usuário, de norma contida neste Ato, para os fins previstos na Lei Estadual n.º 6.677/94.

Art. 55 - As dúvidas de interpretação deste Ato, bem como os casos omissos, serão dirimidas pelo Comitê de Segurança da Informação do Tribunal ou por Comissão instituída pela Presidência do TCE/BA.

Art. 56 – Fica revogado o Ato n.º 291, de 25/08/2000, publicado no DOE de 26 e 27 de agosto de 2000, bem como toda as demais disposições em contrário a esta Norma.

Art. 57 – O Anexo 01 – Glossário é parte integrante desta norma.

Art. 58 - Este Ato entra em vigor na data de sua publicação.

Ridalva Figueiredo
Conselheira Presidente

Anexo 01 – Glossário

Ativo -	Qualquer coisa que tenha valor para a organização.
Autenticação de usuário -	É um processo que busca verificar a identidade do usuário de um sistema, normalmente, no momento em que ele requisita um acesso em um programa ou computador.
Conta de Usuário -	É um código que identifica uma credencial de acesso em um determinado sistema de controle de acesso lógico. É sinônimo de USER_ID, Login, Nome de Usuário, etc. Uma Conta é composta por duas partes: o Código, que é público, e a Senha, que é de conhecimento exclusivo do seu proprietário.
Cyberbullying -	É a prática que envolve o uso de tecnologias de informação e comunicação para dar apoio a comportamentos deliberados, repetidos e hostis praticados por um indivíduo ou grupo com a intenção de prejudicar ou expor negativamente a outrem
Download -	É a transferência de dados de um computador remoto para um computador local.
Firewall -	Sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes.
Incidente de segurança -	Um simples ou uma série de eventos indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
Internet -	Consiste de milhares de redes de computadores privadas interconectadas mundialmente. Pela sua abrangência e facilidade de uso, tem sido usada como plataforma para a prestação de um crescente número de serviços.
Segurança da informação -	Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas
Senha -	São palavras ou sequência de caracteres que funcionam como chaves para o acesso aos Ativos de Informação. Por essa razão, sua adequada proteção é responsabilidade do proprietário da Conta de Usuário.
Spam -	É o envio de mensagens não solicitadas, em grande número, a destinatários desconhecidos
Trabalho Remoto -	É todo e qualquer acesso feito à rede do TCE/BA, através de uma conexão externa.
Upload -	É a transferência de dados de um computador local para um servidor.

CONCURSO PÚBLICO PARA PROVIMENTO DE VAGAS NO CARGO DE PROCURADOR DO MINISTÉRIO PÚBLICO ESPECIAL JUNTO AO TRIBUNAL DE CONTAS DO ESTADO DA BAHIA
EDITAL Nº 06/2010 – TCE/BA, DE 30 DE AGOSTO DE 2010*

A PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DA BAHIA (TCE/BA) torna pública a