GOVERNO DO ESTADO DA BAHIA
Secretaria da Administração da Bahia

Normas de Segurança da Informação

Versão 3.1

Abril / 2018

GOVERNO DO ESTADO DA BAHIA
Jaques Wagner

CONSELHO DE INFORMÁTICA GOVERNAMENTAL – CIGOV
Componentes:

- *Governador do Estado – presidente*
- *Secretário da Casa Civil – vice-presidente*
- *Secretário da Administração*
- *Secretário da Fazenda*
- *Secretário do Planejamento*
- *Secretário da Ciência, Tecnologia e Inovação*
- *Secretário da Indústria, Comércio e Mineração*

SECRETARIA DA CASA CIVIL
Carlos Palma de Mello

ASSESSORIA DE GESTÃO ESTRATÉGICA DE TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO
Renato Falcão de Almeida Souza

SECRETARIA DA ADMINISTRAÇÃO
Manoel Vitório da Silva Filho

COORDENAÇÃO DE TECNOLOGIAS APLICADAS À GESTÃO PÚBLICA
Andre Luis Peixinho de Miranda

GRUPO TÉCNICO DE SEGURANÇA DA INFORMAÇÃO DO FORTIC
Componentes:

- ***CASA CIVIL*** *Mario Henrique Neves Aguiar da Silva*
- ***SAEB*** *Francisco José Garcia Cousino*
  José Ricardo Palomo Tanajura
  Victor Emmanuel Maia Fonseca
  Nilma Ricardo
- ***SSP*** *Telma Cristina Reis e Rocha*
  Egberto Vilas Boas Lemos Filho
- ***SEFAZ*** *Ednilson Gimenes Rosa*
  Nailton Roque Portela Santos
  Jadson Bitencourt Andrade Oliveira
- ***SEPLAN*** *Valdizio Soares dos Santos*
  Thales José Costa de Almeida
- ***PRODEB*** *Elba Lucia de Carvalho Vieira*
  Rosenildo Santos
- ***EMBASA*** *Júlio César Reis e Rocha*
  Leandro Daumerie de Jesus

COLABORAÇÃO

- Superintendência de Gestão Pública – SGP
- Coordenação de Desenvolvimento de Gestão – CDG
  Componentes:
  - *Rita de Cássia Sá e Freitas*
  - *Marta Larocca Santana Rodrigues*
  - *Adriana de Oliveira e Oliveira*
  - *Daniela Svec Silva Bahia Monteiro*
  - *Raquel Miranda de Carvalho*
- Antonio Carlos da Costa Alves Junior
- Ricardo Veloso Fontoura

GRUPO TÉCNICO DE SEGURANÇA DA INFORMAÇÃO DO FORTIC NA REVISÃO VERSÃO 2.0
Componentes:

- ***CASA CIVIL*** *Mario Henrique Neves Aguiar da Silva*
  Fadia Abder Rahim Abdalla
- ***SAEB*** *Francisco José Garcia Cousino*
  Lindinalva Silva Santos
  Roald Holum Moura
- ***SSP*** *Telma Cristina Reis e Rocha*
- ***SEFAZ*** *Ednilson Gimenes Rosa*
  Nailton Roque Portela Santos
- ***SEPLAN*** *Valdizio Soares dos Santos*
- ***PRODEB*** *Elba Lucia de Carvalho Vieira*
  Rosenildo Santos
- ***EMBASA*** *Júlio César Reis e Rocha*
  Leandro Daumerie de Jesus
- ***SESAB*** *César Cardoso*
- ***DETRAN*** *Cristiane Maria de Jesus Santos*

REVISÃO VERSÃO 3.0

GOVERNO DO ESTADO DA BAHIA
Rui Costa

SECRETARIA DA ADMINISTRAÇÃO
Edelvino da Silva Góes Filho

SUPERINTENDÊNCIA DA GESTÃO E INOVAÇÃO
Elizabeth Maria Orge Lorenzo Menezes

GRUPO TEMÁTICO DE SEGURANÇA DA INFORMAÇÃO DO FORTIC
Componentes:

- ***SAEB*** *Fádia Abder Rahim Abdalla*
  Jamile Bastos Oliveira Pino
  Lindinalva Silva Santos
  Nailton Roque Portela Santos
  Roald Holum Moura
- ***SEFAZ*** *Elmo do Vencimento Baraúna*
  Márcio Fraga de Carvalho
- ***PRODEB*** *Mateus Souza Oliveira*
  Rosenildo Souza Santos
- ***EMBASA*** *Aurivan Sérgio de Jesus Silva*
  Geovana Maia de Souza e Silva Tapioca
- ***SEC*** *Rafael Silva Pereira*
- ***SESAB*** *Antonio Cézar de Oliveira Cardoso*
- ***DETRAN*** *Cristiane Maria de Jesus Santos*

REVISÃO VERSÃO 3.1

Norma 03 - Uso da Internet revisada e atualizada para atender a Instrução Normativa nº 027/2017, expedida em 16 de novembro de 2017, que orienta os órgãos e entidades da Administração Pública do Poder Executivo Estadual quanto aos procedimentos para fomentar o acesso de seus servidores às mídias sociais, disponíveis na Rede Mundial de Computadores - Internet.

GOVERNO DO ESTADO DA BAHIA
Rui Costa

SECRETARIA DA ADMINISTRAÇÃO
Edelvino da Silva Góes Filho

SUPERINTENDÊNCIA DA GESTÃO E INOVAÇÃO
Cristine d'Alva Câmera de Araújo

GRUPO TEMÁTICO DE SEGURANÇA DA INFORMAÇÃO DO FORTIC
Componentes:

- ***SAEB*** *Fádia Abder Rahim Abdalla*
  Fernanda Cutrim dos Santos Kumagai
  Lindinalva Silva Santos
  Roald Holum Moura
  Suane Freitas Coutinho
  Valmir Santos Ferreira Filho
- ***SEFAZ*** *Elmo do Vencimento Baraúna*
- ***PRODEB*** *Rosenildo Souza Santos*
- ***EMBASA*** *Ileana Ferreira*
- ***SESAB*** *Antonio Cézar de Oliveira Cardoso*
- ***SETRE*** *Filipe Marques Barreto*
  Marcos Souza de Almeida
  Plínio Jorge Luz de Matos
- ***MINISTÉRIO PÚBLICO*** *Iaçanã Lima de Jesus Carneiro*

BAHIA. Secretaria da Administração.
Normas de Segurança da Informação. -- versão 3.1. -- Salvador: SAEB; SGI, 2018.

74p.

1. Gestão da Informação – Segurança. 3. Normas. I. Título.

CDU 35.076(060.13)(813.8)

Secretaria da Administração, 2ª avenida, 200, tel: 3115-1628
Centro Administrativo da Bahia, CEP 41745-003, Salvador – Bahia

APRESENTAÇÃO

A Segurança da Informação é um assunto que deve merecer cada vez mais atenção dos Gestores das Organizações que fazem parte da Administração Pública do Estado da Bahia. No mundo atual, a informação é um dos ativos mais importantes das organizações e sua proteção se torna cada vez mais crítica para que elas atinjam seus objetivos da maneira mais eficiente possível.

Como unidade da SAEB, cabe à Superintendência da Gestão e Inovação - SGI, planejar, coordenar, promover, supervisionar, controlar e avaliar as ações de desenvolvimento e modernização tecnológicos do setor público.

Neste sentido, este documento foi elaborado para prover a todos os órgãos e entidades da Administração Pública do Poder Executivo Estadual um conjunto de Normas que auxiliem na Gestão da Segurança da Informação em seus ambientes, elevando, assim, o nível de proteção de suas informações e demais ativos críticos.

SUMÁRIO

INTRODUÇÃO

O cenário tecnológico mundial tem evoluído rapidamente, proporcionando cada vez mais facilidades, tanto no uso e armazenamento das informações, quanto na sua transmissão por redes de computadores privadas ou pela Internet. Essa evolução, no entanto, traz consigo um aumento considerável dos riscos aos ambientes tecnológicos das Organizações e, consequentemente, às informações sob sua responsabilidade. Com isso, medidas devem ser aplicadas para prover garantias a essas informações, buscando resguardar aqueles que são considerados os principais pilares da Segurança da Informação:

Confidencialidade: toda informação, esteja ela em meio eletrônico ou não, deve estar acessível somente a quem tem o direito a este acesso. Mecanismos de processos e tecnologia devem ser implementados buscando satisfazer esta premissa;

Integridade: toda informação trafegada ou armazenada deve ter garantias quanto à sua integridade, assegurando que ela não seja indevidamente alterada ou eliminada;

Disponibilidade: as informações devem estar sempre disponíveis para os usuários que dela necessitarem e que tenham autorização para tal acesso;

Autenticidade: devem ser adotados mecanismos que garantam a autenticidade e rastreabilidade dos usuários na utilização dos recursos computacionais, de forma a tornar possível a identificação dos autores de qualquer ação que seja feita utilizando os sistemas informatizados e meios de comunicação.

Para assegurar todos estes aspectos, é necessário que seja colocado em prática um processo de gestão de segurança da informação. Este processo, baseado na Norma ISO/IEC 27001:2013 ("*Information Technology - Security Techniques - Information Security Management Systems - Requirements*"), é o chamado SGSI - Sistema de Gestão de Segurança da Informação (em Inglês, ISMS - *Information Security Management System)*. O SGSI prevê diversas ações, subprocessos, Normas e Procedimentos de Segurança, praticando a missão de reduzir continuamente os riscos à segurança das informações e aos ativos críticos de uma Organização.

NORMAS DE SEGURANÇA DA INFORMAÇÃO

Um dos componentes mais importantes do processo de Gestão de Segurança da Informação é o conjunto de Normas e Procedimentos que irá guiar os gestores e usuários na produção, manuseio e guarda das informações da Organização.

Este documento traz um conjunto básico de Normas a serem implantadas pelos os órgãos e entidades da Administração Pública do Poder Executivo Estadual, buscando elevar o nível de Segurança da Informação no Estado da Bahia.

Seu objetivo é servir de guia na implementação de processos, mecanismos e procedimentos que visem o fortalecimento da segurança da informação no ambiente corporativo do Estado.

É importante deixar claro que este documento não é exaustivo e trata dos principais aspectos relacionados à garantia da segurança dos ativos das Organizações. Outras Normas podem vir a ser divulgadas pela SAEB, assim como normas específicas podem ser produzidas pelos próprios órgãos e entidades, para uso interno, de forma a complementar este conjunto básico.

Norma 01 – Responsabilidades dos Órgãos

1. Objetivo

Orientar os órgãos e entidades da Administração Pública do Poder Executivo Estadual, que compõem a administração direta, autárquica e fundacional, quanto à utilização das Normas de Segurança da Informação.

2. Definições

Ativos de Tecnologia da Informação: estações de trabalho, servidores, *softwares*, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como processos, pessoas e ambientes.

Gestão de Continuidade de Negócios: processo de gestão que identifica ameaças em potencial e os possíveis impactos às operações de negócio caso essas ameaças se concretizem. Este processo fornece um *framework* para que se construa uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar a reputação e a marca do órgão ou entidade e suas atividades de valor agregado.

Gestão de Riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, incluindo, inclusive, análise, avaliação, tratamento, aceitação e comunicação dos riscos.

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Segurança da Informação: conjunto de processos articulados, que busca a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e ampliar as oportunidades de negócio.

3. Abrangência

Esta Norma e todas as outras Normas contidas neste documento se aplicam aos órgãos e entidades da Administração Pública do Poder Executivo Estadual, que compõem a administração direta, autárquica e fundacional. As empresas públicas e sociedades de economia mista poderão adotar os procedimentos contidos nestas Normas.

4. Diretrizes

4.1 Compete à Secretaria da Administração – **SAEB**, por intermédio da Superintendência da Gestão e Inovação – **SGI**:

4.1.1 gerenciar as atividades e projetos de Segurança da Informação:

4.1.1.1 deliberar sobre estratégias, programas e planos de Segurança da Informação;

4.1.1.2 elaborar propostas de Projetos de Segurança da Informação;

4.1.1.3 coordenar ações de Segurança da Informação que envolvam os órgãos e entidades da Administração do Poder Executivo Estadual;

4.1.1.4 mobilizar a Alta Administração e os gestores dos órgãos e entidades da Administração do Poder Executivo Estadual para o cumprimento da Política de Segurança da Informação e a participação destes na implementação de soluções de segurança.

4.1.2 apreciar e validar as proposições do Comitê dos Gestores de Tecnologias de Informação e Comunicação do Estado da Bahia – FORTIC, referentes às normas e Política de Segurança da Informação da Administração Pública do Poder Executivo Estadual:

4.1.2.1 estabelecer diretrizes para a formulação da Política de Segurança da Informação;

4.1.2.2 apreciar matérias que subsidiem o estabelecimento de políticas e estratégias para a Segurança da Informação da Administração Pública do Poder Executivo Estadual;

4.1.2.3 aprovar normas relativas à Segurança da Informação.

4.1.3 difundir e promover o cumprimento das metodologias e boas práticas, em conformidade com as normas e Política de Segurança da Informação;

4.1.4 elaborar e coordenar programas destinados à conscientização e à capacitação em segurança da informação:

4.1.4.1 divulgar os principais aspectos da Segurança da Informação.

4.1.5 avaliar as informações sobre monitoramento do ambiente tecnológico dos órgãos e entidades da Administração do Poder Executivo Estadual e incidentes detectados pela PRODEB:

4.1.5.1 desenvolver, definir e divulgar indicadores de Segurança da Informação;

4.1.5.2 acompanhar e avaliar os indicadores de Segurança da Informação definidos para o Governo do Estado da Bahia;

4.1.5.3 consolidar e emitir os relatórios de incidentes de Segurança da Informação dos órgãos e entidades;

4.1.5.4 analisar informações de incidentes de Segurança da Informação;

4.1.5.5 propor ações para tratamento de incidentes de Segurança da Informação e mitigação de riscos;

4.1.5.6 avaliar as informações sobre o monitoramento do ambiente tecnológico e incidentes de Segurança da Informação detectados pela PRODEB.

4.1.6 propor adoção de soluções de Segurança da Informação existentes no mercado;

4.1.7 prover e manter a ferramenta de Gerenciamento de Riscos, disponibilizada pela SGI/SAEB, utilizada pelos órgãos e entidades da Administração Pública do Poder Executivo Estadual:

4.1.7.1 capacitação na operacionalização da ferramenta de gestão de riscos para a Segurança da Informação.

4.2 Compete às Assessorias de Planejamento e Gestão, por intermédio das Coordenações de Gestão Organizacional e TIC, ou Unidades equivalentes dos órgãos e entidades:

4.2.1 fornecer as diretrizes estratégicas do negócio para orientar as atividades de Segurança da Informação;

4.2.2 prover os recursos humanos, materiais e financeiros para as atividades de Segurança da Informação;

4.2.3 acompanhar, periodicamente, a evolução dos indicadores de Segurança da Informação adotados no âmbito dos respectivos órgãos e entidades;

4.2.4 apoiar, sugerir, garantir e implementar em sua área de atuação as ações de Segurança da Informação;

4.2.5 fazer cumprir a Política e Normas de Segurança da Informação;

4.2.6 reportar a ocorrência de incidentes de Segurança da Informação à SGI.

4.3 Para a execução das atividades de Segurança da Informação, nos órgãos e entidades da Administração Pública do Poder Executivo Estadual, deverão ser observadas todas as demais normas disponibilizadas neste documento e o **Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual**, disponível no site: http://www.fortic.ba.gov.br.

4.4 Caberá a SAEB/SGI analisar e dirimir as dúvidas sobre as Normas e os casos omissos deverão ser encaminhados ao FORTIC para exame.

5. Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.
- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.

5. Data de Revisão

- 23/11/2015

Norma 02 - Classificação da Informação

1. Objetivo

Estabelecer diretrizes que garantam que todas as informações, independente de seus meios de armazenamento ou transmissão, recebam níveis adequados de proteção e sejam classificadas com clara indicação do assunto, fundamento da classificação, indicação do prazo do sigilo e identificação da autoridade que a classificou, respeitando o princípio da observância da publicidade como preceito geral e do sigilo como exceção, conforme a Lei Federal nº 12.527, de 18 de Novembro de 2011 (Lei de Acesso à Informação Pública).

2. Definições

Custodiante da Informação: aquele que armazena, processa, veicula e trata a informação, mediante orientação dada pela classificação da informação e assume, em conjunto com o proprietário da informação, a responsabilidade pela proteção desta.

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação Pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Proprietário da Informação: aquele que gera ou adquire a informação.

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os usuários das informações custodiadas ou de propriedade da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 A informação em poder dos órgãos e entidades, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada no grau **Ultrassecreto, Secreto** ou **Reservado**

4.2 Para a classificação da informação em grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

4.2.1 a gravidade do risco ou dano à segurança da sociedade e do Estado; e

4.2.2 o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.

4.3 São passíveis de classificação no grau **Ultrassecreto**, **Secreto** ou **Reservado** as informações consideradas imprescindíveis à segurança da sociedade ou do Estado, cuja divulgação ou acesso irrestrito possa:

4.3.1 pôr em risco a defesa e a integridade do território estadual;

4.3.2 prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do Estado, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

4.3.3 pôr em risco a vida, a segurança ou a saúde da população;

4.3.4 oferecer elevado risco à estabilidade financeira, econômica ou monetária do Estado;

4.3.5 prejudicar ou causar risco a planos ou operações estratégicos dos órgãos de Segurança do Estado;

4.3.6 prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico do Estado;

4.3.7 por em risco a segurança de instituições ou de altas autoridades nacionais, estaduais ou estrangeiras e seus familiares;

4.3.8 comprometer atividades de inteligência, de investigação ou de fiscalização em andamento, relacionadas com prevenção ou repressão de infrações.

4.4 Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista, devem vigorar, a partir da data de sua produção, nos seguintes parâmetros:

4.4.1 **Ultrassecreta:** 25 (vinte e cinco) anos;

4.4.2 **Secreta:** 15 (quinze) anos;

4.4.3 **Reservada:** 5 (cinco) anos.

4.5 O prazo de sigilo das informações classificadas no grau **Ultrassecreto** poderá ser prorrogado por uma única vez e por período determinado não superior a vinte e cinco anos, enquanto seu acesso ou divulgação puder ocasionar ameaça externa à integridade do território nacional ou grave risco às relações internacionais do Estado.

4.6 As informações que puderem colocar em risco a segurança do Governador e Vice Governador do Estado e respectivos cônjuges e filhos (as) deverão ser, automaticamente, consideradas como **Reservadas** e ficar sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

4.7 As informações que não forem classificadas como **Ultrassecretas**, **Secretas** ou **Reservadas** deverão ser consideradas, automaticamente, como Públicas, resguardadas as exceções legalmente previstas como sigilo, a exemplo de:

4.7.1 sigilo fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial e segredo de justiça;

4.7.2 informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

4.8 Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, a informação deverá ser considerada automaticamente classificada como Pública, respeitadas as exceções previstas nesta norma.

5. Recomendações para Classificação

5.1 Informação "pessoal" não é considerada uma classificação, mas uma designação para uma informação relacionada à pessoa natural identificada ou identificável relativa à intimidade, vida privada, honra e imagem, significando que a informação é direcionada e que somente o destinatário e as pessoas expressamente autorizadas por ele podem ter acesso.

5.2 Toda informação deve possuir um rótulo com a sua classificação. As informações não rotuladas serão classificadas, automaticamente, como "Públicas", ressalvadas as exceções previstas nesta norma.

5.3 A classificação das informações deve ser feita para determinar as medidas de proteção necessárias, visando atender as diretrizes da Lei de Acesso à Informação Pública e otimizar os custos com a sua proteção e disponibilização.

5.4 A classificação deve ser realizada no momento em que a informação é gerada ou adquirida, conforme as seguintes competências:

5.4.1 **Grau Ultrassecreto:** Governador e Vice Governador do Estado;

5.4.2 **Grau Secreto:** além dos previstos no item 5.4.1, também, os Secretários de Estado e as autoridades com as mesmas prerrogativas, Comandantes da Polícia Militar e os titulares máximos de autarquias, fundações ou empresas públicas e sociedades de economia mista;

5.4.3 **Grau Reservado:** além dos previstos nos itens 5.4.1 e 5.4.2, também aqueles que exerçam funções de direção, comando ou chefia, no nível DAS-2A ou superior, do Grupo-Direção e Assessoramento Superior ou hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade.

5.5 A competência prevista nos itens 5.4.1 e 5.4.2 poderá ser delegada expressamente pela autoridade responsável a agente público, inclusive em missão no exterior, vedada a subdelegação.

5.6 O proprietário pode solicitar apoio técnico à Superintendência da Gestão e Inovação – SGI, através da Coordenação de Segurança da Informação, caso existam dificuldades ou dúvidas acerca da classificação a ser dada a uma informação.

5.7 A informação deve receber tratamento adequado à sua classificação durante todo o seu ciclo de vida.

5.8 A inexistência de classificação explícita não exime o proprietário, os custodiantes e os usuários das suas responsabilidades quanto a avaliar o nível de sensibilidade da informação.

5.9 Os órgãos e entidades da Administração Pública do Poder Executivo Estadual deverão reavaliar as informações classificadas no grau **Ultrassecreta** e **Secreto**, no prazo máximo de **dois** anos.

5.10 Enquanto não transcorrido o prazo de reavaliação previsto no item 5.9, será mantida a classificação da informação, observados os prazos e disposições desta norma.

5.11 As informações classificadas no grau **Ultrassecreto** e **Secreto** não reavaliadas no prazo previsto no item 5.9 serão consideradas, automaticamente, de acesso público.

5.12 As informações classificadas no grau **Ultrassecreto**, **Secreto** e **Reservado** deverão conter:

5.12.1 código de indexação de documento;

5.12.2 categoria na qual se enquadra a informação;

5.12.3 indicação de dispositivo legal que fundamenta a classificação;

5.12.4 data da produção, data da classificação e prazo da classificação.

5.13 É expressamente proibida aos usuários a utilização, repasse e/ou divulgação indevida de toda e qualquer informação de propriedade da Administração Pública do Poder Executivo Estadual, exceto nas hipóteses previstas na Lei Federal nº 12.527, de 18 de Novembro de 2011.

5.14 Antes que informações custodiadas ou de propriedade da Administração Pública do Poder Executivo Estadual sejam disponibilizadas a terceiros, estes devem ser orientados e supervisionados quanto aos aspectos da segurança da informação. A Administração Pública do Poder Executivo Estadual deve garantir que o compromisso de sigilo seja parte integrante do contrato.

5.15 Informações **Reservadas**, **Secretas** ou **Ultrassecretas** não devem ser descartadas como lixo comum. Documentos impressos ou em mídia eletrônica, que contenham informação com esses níveis de classificação, devem ser destruídos antes de serem descartados, de forma que torne impossível a sua recuperação.

6. Competências

6.1 **Usuário**:

6.1.1 Aplicar o tratamento adequado à informação, de acordo com os níveis definidos nesta norma.

6.2 **Autoridades previstas no item 5.5 desta norma**:

6.2.1 Classificar as informações, conforme as diretrizes desta norma.

6.3 **Proprietário da Informação**:

6.3.1 Determinar o nível de criticidade e a classificação correta das informações utilizadas nos ativos sob sua responsabilidade, de forma a subsidiar as decisões de classificação a serem aplicadas pelos entes competentes.

7. Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.
- Lei Federal nº 12.527, de 18 de Novembro de 2011 – Lei Federal de Acesso à Informação Pública.

8. Data de Revisão

- 23/11/2015

Norma 03 - Uso da Internet

1. Objetivo

Estabelecer as diretrizes de proteção relativas ao uso da *Internet* e de outras redes públicas de computadores, com o objetivo de reduzir o risco a que estão expostos os Ativos de Tecnologia da Informação da Administração Pública do Poder Executivo Estadual, tendo em vista que a *Internet* tem sido veículo de muitas ações prejudiciais às organizações, gerando perdas financeiras, perdas de produtividade, danos aos sistemas e à imagem da organização, entre outras consequências.

2. Definições

Ativos de Tecnologia da Informação: estações de trabalho, servidores, *softwares*, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como processos, pessoas e ambientes.

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre.

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Internet: consiste de milhares de redes de computadores interconectadas mundialmente e que pela sua abrangência e facilidade de uso, tem sido usada como plataforma para a prestação de um crescente número de serviços.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

Mídias Sociais – são plataformas baseadas em Internet que disponibilizam informações, notícias e quaisquer tipos de conteúdo, que permitem a interação entre pessoas, possibilitando o compartilhamento de imagens, vídeos, experiências, pensamentos, entre outros.

3. Abrangência

Esta Norma se aplica a todos os usuários que fazem uso da Internet, permanente ou temporariamente, através dos recursos computacionais disponibilizados pela Administração Pública do Poder Executivo Estadual, bem como os que utilizam a Internet como meio de comunicação através de conexão com a rede interna da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Toda área de transferência de dados em computadores da Administração Pública do Poder Executivo Estadual acessível pela Internet e disponível publicamente para gravação deve ser limpa regularmente.

4.2 A informação obtida na Internet de forma livre e gratuita deve ser confirmada por fontes fidedignas antes de ser efetivamente usada.

4.3 A Administração Pública do Poder Executivo Estadual pode examinar, sem aviso prévio, o conteúdo de *cache* de navegadores Web, favoritos, histórico de sites visitados, configurações dos *softwares* e outras informações armazenadas ou transmitidas pelos seus computadores.

4.4 Os Ativos de Tecnologia da Informação da Administração Pública do Poder Executivo Estadual, incluindo as conexões com a Internet, *hardware* e *software*, devem ser empregados na consecução dos seus objetivos, sendo vedada a sua utilização para outros fins, exceto para os casos explicitamente permitidos por esta norma.

4.5 Controles de Acesso a Serviços da Internet

4.5.1 A permissão de acesso à Internet deve ser seletiva em relação aos serviços disponibilizados e ser concedida exclusivamente àqueles usuários que necessitem deste acesso para o seu trabalho, podendo ser removida quando não for mais necessária.

4.5.2 O acesso à Internet deve ser disponibilizado por meio de listas positivas ou negativas, cabendo a cada unidade definir suas regras.

4.5.3 A permissão de acesso à Internet deve ser concedida através de uma Conta de Usuário que possibilite identificar, individualmente, seu proprietário, podendo o histórico de acesso, inclusive o conteúdo, ser monitorado, sem necessidade de notificação prévia, devendo ser armazenado por um período mínimo de 90 (noventa) dias, ou quando cabível, por período previsto em lei.

4.5.4 Não é permitido suprimir, omitir ou mascarar a identificação da Conta de Usuário a qualquer serviço da Internet, exceto para os serviços que permitem apenas conexão anônima, não sendo permitido também o uso de mecanismos de dissimulação do usuário, como *remailers*, IP *Spoofing* e tradutores de URL.

4.5.5 A Administração Pública do Poder Executivo Estadual pode, sem aviso prévio, restringir o acesso a serviços da Internet, tais como sítios *Web*, redes de dados ponto a ponto e *download* de arquivos.

4.5.6 A possibilidade de acessar qualquer serviço da Internet não implica em autorização para acessá-lo.

4.6 Conexões de Rede com a Internet

4.6.1 É vedada a conexão entre qualquer rede de dados da Administração Pública do Poder Executivo Estadual e a Internet através de serviços de telecomunicações não autorizados pela área de TIC do órgão ou entidade.

4.6.2 É vedada a utilização de dispositivos de acesso à *Internet* não autorizados pela área de Tecnologia da Informação dos órgãos ou entidades, em equipamentos pertencentes à Administração Pública do Poder Executivo Estadual.

4.6.3 Toda comunicação entre computadores remotos e as redes da Administração Pública do Poder Executivo Estadual, através da *Internet* ou outra rede pública, deve ser autenticada e criptografada, usando soluções tecnológicas autorizadas pelo órgão ou entidade responsável pela rede, com exceção do acesso aos sítios *Web* públicos da Administração Pública do Poder Executivo Estadual.

4.6.4 Toda a comunicação entre as redes da Administração Pública do Poder Executivo Estadual e a *Internet* ou qualquer outra rede pública deve necessariamente passar por *firewall*, configurado com política restritiva, com monitoramento bidirecional dos fluxos de comunicação e com proteção contra ataques cibernéticos.

4.7 Uso Aceitável da *Internet*

4.7.1 É permitido o uso de mídias sociais, cabendo a cada unidade definir suas regras de acesso.

4.7.2 É permitido o acesso a sites que sejam fontes de informação necessária à execução das atividades da Administração Pública do Poder Executivo Estadual.

4.7.3 É permitido o uso de serviços pessoais prestados através da *Internet*, tais como banco *on-line*, reservas de passagens, serviços de órgãos públicos, entre outros, limitados ao estritamente necessário, nos horários estabelecidos pelas áreas de Tecnologia da Informação dos órgãos e entidades da Administração Pública do Poder Executivo Estadual.

4.7.4 É permitido o uso de serviço de mensagem instantânea por meio da ferramenta corporativa do Poder Executivo Estadual.

4.7.5 Não devem ser usados os recursos de "Salvar Senha" ou "Lembrar Senha", disponíveis na maioria das aplicações (*Outlook, Internet Explorer,* etc.), devendo ser desmarcada sempre que for apresentada esta opção. Senhas não devem ser incluídas em nenhum outro processo de autenticação automática disponível.

4.7.6 Quando estiver usando a *Internet* e verificar que o site acessado contém conteúdo impróprio, o usuário deve abandonar o site e abrir um incidente de Segurança da Informação.

4.7.7 Não é permitido o uso de aplicações ponto a ponto (*peer-to-peer*) para distribuição de arquivos.

4.7.8 Não é permitido o uso de jogos *on-line*.

4.7.9 Ressalvados os interesses da Administração Pública do Poder Executivo Estadual, não é permitido:

a) o acesso e/ou a publicação de conteúdos impróprios, que são aqueles relativos à pornografia, racismo, violência, incitação ao ódio, invasão de computadores, jogos, entre outros;

b) o uso de serviços de mensagem instantânea, seja por software específico ou via Web;

c) o uso de serviços de áudio e vídeo em tempo real, tais como rádio on-line, TV on-line e telefonia IP;

d) a sondagem, investigação ou teste de vulnerabilidade em computadores e sistemas da Administração Pública do Poder Executivo Estadual ou de qualquer outra organização, exceto quando autorizada pela área de Tecnologia da Informação do respectivo órgão ou entidade da Administração Pública;

e) o uso ou a posse de ferramentas de hardware e software para sondagem, análise de vulnerabilidade, monitoramento de rede, comprometimento de sistemas, ataques e captura de dados, exceto quando autorizado pela área de Tecnologia da Informação do respectivo órgão ou entidade da Administração Pública do Poder Executivo Estadual.

4.8 Uso Corporativo de Mídias Sociais

4.8.1 Regras básicas de boa convivência, de educação, adotadas dentro do órgão ou entidade, também são válidas para ambientes virtuais;

4.8.2 Participar de mídias sociais é um ato de caráter público. O usuário será responsável por tudo que publicar, compartilhar, curtir, comentar, entre outros, devendo estar ciente que na Internet tudo fica registrado podendo ser rastreado;

4.8.3 Quando utilizadas para fins profissionais, é recomendável prudência em relação ao conteúdo publicado e compartilhado;

4.8.4 Não é permitido:

a) Criar perfis com nomes que façam menção ao órgão ou entidade e ao Governo Estadual sem autorização da Assessoria de Comunicação, ou unidade equivalente;

b) Falar em nome do órgão ou entidade, a não ser que seja autorizado oficialmente;

c) Vincular sua conta de e-mail corporativo a contas pessoais em mídias sociais;

d) Responder a ataques ou provocações nas mídias sociais envolvendo o nome do órgão/entidade. Neste caso, o colaborador deve informar o fato ao gestor imediato ou à Assessoria de Comunicação;

e) Fazer qualquer tipo de manifestação ou emitir opinião que possa ser considerada ambígua, discriminatória, caluniosa, difamatória, agressiva ou hostil;

f) Divulgar informações classificadas como sigilosa ou internas para o órgão/entidade, ou sobre a vida pessoal de colaboradores;

g) Participar de grupos ou discussões relacionadas a assuntos de cunho negativo ao órgão/entidade e ao local de trabalho;

h) Emitir opinião negativa ou publicar mensagens de conteúdo ofensivo, ou moralmente questionável, sobre qualquer área ou colaboradores da órgão/entidade;

i) Postar ou emitir manifestações partidárias, como endosso a campanhas políticas, declarar apoio a partidos políticos ou políticos de qualquer partido.

4.9 Criptografia

4.9.1 Recomenda-se que toda a informação classificada como sigilosa, transmitida pela *Internet*, deve ser criptografada, conforme padrões de criptografia homologados pela área de Tecnologia da Informação do respectivo órgão ou entidade da Administração Pública do Poder Executivo Estadual.

4.9.2 Informações que são alvo típico de criminosos, tais como senhas de contas bancárias, números de cartões de crédito, senhas de sistemas, entre outras, não devem ser publicadas na *Internet* ou transmitidas via Correio Eletrônico sem criptografia.

4.10 Legalidade

4.10.1 Sempre que as transações através da *Internet* ultrapassarem as fronteiras nacionais, devem ser observadas as legislações internacionais pertinentes.

4.10.2 A propriedade intelectual deve ser respeitada em qualquer atividade e sempre que os recursos computacionais da Administração Pública do Poder Executivo Estadual estiverem sendo usados. A reprodução ou encaminhamento de qualquer conteúdo protegido por direitos de propriedade requer a autorização do proprietário dos direitos autorais.

4.10.3 Sempre que informações obtidas da *Internet* forem usadas em documentos internos, a fonte deve ser citada.

4.10.4 A indicação de direitos reservados deve ser presumida para todo conteúdo disponível na *Internet*, a menos que contenha informação contrária.

4.10.5 Usuários dos serviços de *Internet* da Administração Pública do Poder Executivo Estadual não devem obter, armazenar ou transmitir conteúdo ilegal, tais como *software* não licenciado, pornografia infantil, senhas, informações bancárias extraviadas, entre outros.

4.11 *Download* de Arquivos

4.11.1 Não é permitido o *download* de filmes, músicas, vídeo *clips* ou conteúdos semelhantes relacionados a entretenimento, ressalvado os interesses da

Administração Pública do Poder Executivo Estadual, desde que os mesmos não sejam protegidos por direitos autorais.

4.11.2 O *download* de arquivos 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.

4.11.3 O *download* de *softwares* deve obedecer aos contratos estabelecidos com os fornecedores, quando aplicável.

4.11.4 Todo arquivo obtido em fontes externas à Administração Pública do Poder Executivo Estadual deve ser submetido à verificação de *software* antivírus antes de ser utilizado.

5. Competências

5.1 **Área de Tecnologia da Informação do Órgão ou Entidade**:

5.1.1 prover os recursos necessários ao cumprimento desta Norma;

5.1.2 avaliar e homologar novos serviços de *Internet* antes de serem utilizados.

6. Documentos relacionados

- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.
- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.
- Norma 02 - Classificação da Informação.
- Norma 16 - Proteção Contra Código Malicioso.
- Norma 05 - Acesso e Utilização do Correio Eletrônico.
- Norma 11 - Intercâmbio de Informações.
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

7. Data de Revisão

- 29/03/2018

Norma 04 - Acesso aos Recursos de Tecnologia da Informação

1. Objetivo

Estabelecer as diretrizes e responsabilidades para o acesso aos recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual.

2. Definições

Autenticação: processo de verificação que confirma se uma entidade ou um objeto é quem ou o que afirma ser, incluindo, em alguns exemplos, a confirmação da origem e da integridade das informações, tal como a verificação de uma assinatura digital ou da identidade de um utilizador ou de um computador.

Conta de Usuário: credencial de acesso à rede ou sistemas, de uso pessoal, intransferível e de responsabilidade de seu usuário designado.

Conta Genérica: credencial de acesso à rede que não identifica o usuário que a utiliza.

Credencial de Acesso: elemento utilizado para autenticar um usuário perante recursos de Tecnologia da Informação, tais como nome de usuário e senha, certificado digital, informação biométrica ou equivalentes.

Estação de Trabalho: todos os computadores e equipamentos correlatos da Administração Pública do Poder Executivo Estadual, inclusive dispositivos móveis.

Login/Logon: processo de autenticação com o objetivo de permitir o uso de um sistema computacional ou recursos de rede de forma segura.

Logoff: processo de encerramento do uso de um sistema computacional ou recursos de rede, removendo as credenciais de acesso.

Recursos de Tecnologia da Informação: estações de trabalho, servidores, redes, sistemas, serviços, banco de dados e dispositivos de interconexão.

Rede: estações de trabalho, servidores e outros dispositivos interligados que compartilham informações ou recursos da Administração Pública do Poder Executivo Estadual.

Smartcard: cartão de plástico com um microprocessador embutido, que utiliza criptografia para aplicar princípios da Segurança da Informação como: integridade, autenticidade e não repúdio.

Token: dispositivo, que juntamente com algo que o usuário conhece, como uma senha, vai autorizar o acesso a um sistema ou rede de computadores.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os usuários de informações ou recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Concessão de Acesso

4.1.1 A licença para a utilização dos recursos de Tecnologia da Informação é uma concessão da Administração Pública do Poder Executivo Estadual aos usuários que necessitem deles para desempenhar suas funções. A utilização poderá ser monitorada em tempo real e a licença poderá ser suspensa a qualquer momento por decisão do Gestor da área do usuário, da área de Tecnologia da Informação do órgão ou entidade, de acordo com os exclusivos critérios destes, visando evitar perda de produtividade e riscos de segurança.

4.1.2 O acesso à consulta ou utilização dos recursos de Tecnologia da Informação é permitido após a identificação do usuário, somente por meio de suas próprias credenciais de acesso.

4.1.3 As credencias de acesso aos recursos de Tecnologia da Informação são pessoais, intransferíveis e de responsabilidade exclusiva do usuário, exceto para aqueles recursos que não suportarem a criação de credenciais individuais.

4.1.4 Toda solicitação, alteração, bloqueio e desbloqueio de acesso aos recursos de Tecnologia da Informação ou aos sistemas deve ser documentada.

4.1.5 O Gestor da área do usuário deve informar à área de Tecnologia da Informação do órgão ou entidade ou ao administrador do recurso de Tecnologia da Informação todos os direitos de acesso que o usuário deve possuir.

4.1.6 Todos os direitos de acesso aos recursos de Tecnologia da Informação devem ter prazo de vigência definido.

4.1.7 É expressamente proibida qualquer tentativa de acesso não autorizado aos recursos de Tecnologia da Informação.

4.1.8 A utilização de contas genéricas deve ser limitada ao estritamente necessário.

4.1.9 Os órgãos e entidades da Administração Pública do Poder Executivo Estadual que disponibilizem o acesso a recursos de Tecnologia da Informação ao cidadão devem desenvolver e comunicar regulamento específico para o bom uso desses recursos.

4.2 Conexão de Equipamentos

4.2.1 Somente dispositivos autorizados pela área de Tecnologia da Informação do órgão ou entidade poderão ter acesso aos recursos de rede da Administração Pública do Poder Executivo Estadual.

4.3 Gerenciamento de Senhas

4.3.1 A elaboração de senhas para acesso à rede ou aos sistemas deve ser realizada conforme procedimento estabelecido pela área de Tecnologia da Informação do órgão ou entidade, o qual deve prever troca periódica de senhas, senhas de difícil dedução e bloqueio automático da sessão por inatividade.

4.3.2 Todas as contas de usuário devem ter suas senhas alteradas no primeiro *logon* na rede e nos sistemas de informação, para assegurar sua confidencialidade.

4.3.3 Os critérios para elaboração, manutenção e gerenciamento dos acessos devem levar em consideração a criticidade das informações e as necessidades dos processos de negócio envolvidos.

4.4 Análise Crítica

4.4.1 Os direitos de acesso dos usuários à rede e aos sistemas devem ser revisados periodicamente.

4.4.2 Os direitos de acesso dos usuários em afastamento definitivo da organização devem ser revogados.

4.4.3 Os direitos de acesso dos usuários em afastamento temporário devem ser suspensos no período da ausência.

4.4.4 Os direitos de acesso dos usuários em transferência de área devem ser revistos.

5. Competências

5.1 Área de Tecnologia da Informação do Órgão ou Entidade:

5.1.1 administrar os acessos à rede e aos sistemas da Administração Pública do Poder Executivo Estadual;

5.1.2 elaborar procedimento de gerenciamento de senhas em consonância com a criticidade das informações e as necessidades dos processos de negócio envolvidos.

5.2 Gestor da Área do Usuário

5.2.1 comunicar à área de Tecnologia da Informação do órgão ou entidade todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos;

5.2.2 comunicar à área de Tecnologia da Informação do órgão ou entidade sempre que tomar ciência de direitos de acesso desnecessários à execução das atividades por parte de seus subordinados ou de terceiros.

5.3 Usuário

5.3.1 manter sigilo da senha de acesso à rede e aos sistemas, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de acesso;

5.3.2 não compartilhar com terceiros sua credencial de acesso à rede ou aos sistemas;

5.3.3 informar ao seu Gestor quando forem identificados direitos de acesso desnecessários à execução das suas atividades profissionais;

5.3.4 bloquear sua estação de trabalho ou efetuar *logoff* da rede sempre que se ausentar de sua área de trabalho;

5.3.5 comunicar, imediatamente, à área de Tecnologia da Informação do órgão ou entidade qualquer ocorrência de perda ou avaria de dispositivos adicionais de autenticação, tais como *tokens*, *smartcards* e outros.

6. Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.
- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.
- Norma 16 - Proteção Contra Código Malicioso.
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 03 - Uso da Internet.

7. Data de Revisão

- 23/11/2015

Norma 05 - Acesso e Utilização do Correio Eletrônico

1. Objetivo

Definir as diretrizes de acesso e utilização segura do Correio Eletrônico disponibilizado pela Administração Pública do Poder Executivo Estadual.

2. Definições

E-mail: forma reduzida para *E(lectronic) Mail* - Correio Eletrônico.

***Hiperlink*:** palavras ou endereços em destaque de uma página da *Internet* ou mensagem de Correio Eletrônico que, ao serem clicadas, efetuam o direcionamento para outra parte do texto da mensagem ou página da *Internet*.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

Webmail: é uma interface da *Internet* que permite consultar e enviar Correio Eletrônico (*E-mail).*

3. Abrangência

Esta Norma se aplica a todos os usuários que utilizam o serviço de Correio Eletrônico disponibilizado pela Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 O serviço de *Correio Eletrônico* corporativo é uma concessão da Administração Pública do Poder Executivo Estadual, sendo assim, seu uso é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens não relacionadas às atividades profissionais, a exemplo de, mas não limitado a:

4.1.1 assuntos que provoquem assédio, constrangimento ou que prejudiquem a imagem da organização;

4.1.2 temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético;

4.1.3 fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais da organização.

4.2 As permissões de acesso a serviços de *e-mail* particulares, tais como *webmail*, podem ser estabelecidas e gerenciadas pela área de Tecnologia da Informação do órgão ou entidade e pelas áreas de negócio, em função dos interesses da Administração Pública;

4.3 O acesso ao Correio Eletrônico corporativo se dará, minimamente, pelo conjunto "Identificação do Usuário e Senha", que é pessoal e intransferível.

4.4 O endereço de *e-mail* disponibilizado ao usuário é de uso pessoal e intransferível e de responsabilidade do mesmo. Portanto, é terminantemente proibido suprimir, modificar ou substituir a identidade do remetente de uma mensagem do Correio Eletrônico.

4.5 Havendo indícios de que mensagens veiculadas pelo correio eletrônico possam ocasionar quebra de segurança ou violação de quaisquer das vedações constantes deste ou de outro ato normativo, a área de Tecnologia da Informação do órgão ou entidade responsável pela administração do Serviço de Correio Eletrônico adotará, imediatamente, medidas para a apuração dessas irregularidades, utilizando-se dos meios e procedimentos legalmente previstos.

4.6 A disponibilização do Correio Eletrônico pode ser suspensa a qualquer momento por decisão do Gestor da área do usuário ou da área de Tecnologia da Informação do órgão ou entidade.

4.7 As concessões e revogações de acesso ao serviço de Correio Eletrônico devem ser autorizadas pelo Gestor da área do usuário por meio de uma solicitação de serviço à área de Tecnologia da Informação do órgão ou entidade.

4.8 Os anexos e/ou *hiperlinks* das mensagens de Correio Eletrônico poderão ser bloqueados quando oferecerem riscos à Segurança da Informação.

4.9 A abertura de mensagens de remetentes desconhecidos, externos à Administração Pública do Poder Executivo Estadual, deve ser avaliada, especialmente quando houver dúvidas quanto à natureza do seu conteúdo, como arquivos anexados não esperados ou *hiperlinks* para endereços externos não relacionados às atividades profissionais em curso.

4.10 A quantidade de destinatários deve ser limitada por mensagem, com o objetivo de coibir a prática de Spam. Cabe à área de Tecnologia da Informação do órgão ou entidade estabelecer tal limite, bem como acordar com as áreas de negócio as eventuais exceções, de acordo com os interesses da Administração Pública.

4.11 Todas as mensagens originárias de usuários da Administração Pública do Poder Executivo Estadual deverão conter a assinatura do remetente em formato padronizado, além de um aviso legal, também padronizado, referenciando a confidencialidade da informação. Esses padrões devem ser definidos pela Superintendência da Gestão e Inovação - SGI.

4.12 Limites de armazenamento das caixas de Correio Eletrônico devem ser estabelecidos pela área de Tecnologia da Informação do órgão ou entidade, considerando as necessidades dos processos de negócio que o serviço de Correio Eletrônico suporta, bem como limitações técnicas aplicáveis.

5. Competências

5.1 Área de Tecnologia da Informação do Órgão ou Entidade:

5.1.1 conceder, suspender e revogar os acessos ao serviço de Correio Eletrônico;

5.1.2 administrar as funcionalidades e a segurança do serviço de Correio Eletrônico.

5.2 Gestor da Área do Usuário:

5.2.1 comunicar à área de Tecnologia da Informação do órgão ou entidade todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos.

5.3 Usuário:

5.3.1 responder pelo uso adequado dos serviços e recursos de Correio Eletrônico a ele disponibilizados, nas suas mais diversas formas de acesso, inclusive por meio de dispositivos móveis, em consonância com esta Norma.

6. Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.
- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.
- Norma 16 - Proteção Contra Código Malicioso.
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 03 - Uso da Internet.

7. Data de Revisão

- 23/11/2015

Norma 06 - Gerenciamento de Incidentes de Segurança da Informação

1. Objetivo

Normatizar o registro e o tratamento de incidentes de Segurança da Informação no âmbito da Administração Pública do Poder Executivo Estadual.

2. Definições

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Log: arquivo que contém informações sobre eventos de qualquer natureza em um sistema computacional, análise forense para a elucidação de incidentes de segurança, auditoria de processos, cumprimento de exigências legais para a manutenção de registro do histórico de acessos ou eventos e para a resolução de problemas (*debugging*).

Usuário: qualquer colaborador seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza os recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os usuários de informações ou recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Todo usuário deve registrar incidentes de Segurança da Informação, conforme orientações descritas em procedimento específico constante do Sistema de Gestão de Segurança da Informação.

4.2 A área de Tecnologia da Informação do órgão ou entidade deve registrar um incidente de Segurança da Informação para toda falha de segurança identificada nos recursos de Tecnologia da Informação da Administração Pública do Poder Executivo Estadual.

4.3 As informações referentes aos responsáveis pelo registro de incidentes de Segurança da Informação são sigilosas, entretanto esta identificação é obrigatória.

4.4 A área de Tecnologia da Informação do órgão ou entidade deve garantir que planos de ação sejam elaborados para tratamento de incidentes, e monitorar sua implementação.

4.5 É vedado ao usuário intervir no tratamento dos incidentes sem a devida autorização ou qualificação.

5. Competências

5.1 Área de Tecnologia da Informação do Órgão ou Entidade:

5.1.1 identificar e documentar incidentes de Segurança da Informação por meio de análise dos logs dos recursos de Tecnologia da Informação;

5.1.2 reportar todos os incidentes de Segurança da Informação à Superintendência da Gestão e Inovação - SGI, de forma regular;

5.1.3 elaborar Planos de Recuperação de Desastres (PRD) para os processos críticos;

5.1.4 executar procedimentos e ações corretivas quando necessário;

5.1.5 informar ao usuário as ações tomadas em relação aos incidentes registrados, quando aplicável.

5.2 Gestor da Área do Usuário:

5.2.1 apoiar a área de Tecnologia da Informação do órgão ou entidade na solução dos incidentes de Segurança da Informação;

5.2.2 apoiar na execução das ações corretivas/preventivas estabelecidas para o tratamento dos incidentes;

5.2.3 apoiar a área de Tecnologia da Informação do órgão ou entidade, na elaboração e implementação dos planos de contingência para diferentes tipos de incidentes de segurança, visando reduzir os impactos, restabelecendo os processos de negócio afetados, o mais rápido possível.

5.3 Usuário:

5.3.1 registrar incidentes de Segurança da Informação.

6. Documentos Relacionados

- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.
- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.
- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.

7. Data de Revisão

- 23/11/2015

Norma 07 - Gerenciamento da Auditoria de Segurança da Informação

1. Objetivo

Definir as diretrizes do processo de Auditoria de Segurança da Informação, no âmbito da Administração Pública do Poder Executivo Estadual.

2. Definições

Alta Administração: dirigente máximo dos órgãos e entidades da Administração Pública do Poder Executivo Estadual, chefes de gabinete, superintendentes e diretores. A Alta Administração dos órgãos e entidades também pode ser proprietária, custodiante ou usuária da informação.

Custodiante da Informação: aquele que armazena, processa, veicula e trata a informação, mediante orientação dada pela classificação e assume, em conjunto com o proprietário da informação, a responsabilidade pela proteção desta.

Proprietário da Informação: aquele que gera ou adquire a informação.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os processos de negócio da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Toda Auditoria de Segurança da Informação deve estar autorizada de acordo com a legislação vigente.

4.2 A necessidade de Auditoria de Segurança da Informação deve ser verificada regularmente, produzindo um relatório de diretrizes de auditoria. Essa verificação deve contemplar, entre outros:

4.2.1 análise dos documentos que compõem a Política de Segurança da Informação;

4.2.2 resultados de auditorias anteriores;

4.2.3 indicadores de Segurança da Informação;

4.2.4 análise dos incidentes de Segurança da Informação registrados;

4.2.5 informações relativas a análises de risco.

4.3 Requisitos e atividades de Auditoria de Segurança da Informação devem ser planejados para minimizar o risco de interrupção dos processos de negócio envolvidos, devendo o planejamento contemplar, dentre outros:

4.3.1 áreas, usuários, processos e sistemas que serão auditados;

4.3.2 controles de Segurança da Informação que serão auditados;

4.3.3 estratégia de comunicação com todos os envolvidos;

4.3.4 identificação dos auditores;

4.3.5 independência dos auditores em relação às atividades auditadas;

4.3.6 cronograma de execução da auditoria.

4.4 Os auditores devem ter acesso apenas à leitura de *software* e dados, só sendo permitido outros acessos por meio de cópias isoladas e estes devem ser apagados ao final da auditoria, ou dada a devida proteção quando houver a obrigação ou necessidade de armazenar tais cópias.

4.5 Quando o acesso a dados sensíveis for indispensável para os objetivos da auditoria, mecanismos adicionais devem ser implementados para garantia de sua confidencialidade.

4.6 Mecanismos que garantam o registro de todas as atividades da auditoria devem ser implementados, de forma a produzir uma trilha de referência.

4.7 O acesso às ferramentas de auditoria deve ser restrito e controlado, visando prevenir uso não autorizado.

4.8 O processo de auditoria deve produzir relatórios contendo, dentre outros, os dados da área, do usuário, o processo ou sistema auditado, os controles verificados, evidências para conformidades e justificativas para não conformidades. Os dados destes relatórios devem alimentar o processo de Gestão de Indicadores de Segurança da Informação.

4.9 Um plano com ações preventivas e corretivas deve ser elaborado com base no relatório gerado pelo processo de auditoria.

4.10 O resultado de auditorias de Segurança da Informação deve ser caracterizado como informação sigilosa quando esse puder comprometer a segurança dos processos de negócio do órgão ou entidade a que se refere.

4.11 Uma análise crítica dos resultados da auditoria deve ser conduzida, com o objetivo de determinar ações de melhoria para possíveis ajustes na Política de Segurança da Informação.

5. Competências

5.1 **Auditor**:

5.1.1 planejar a Auditoria de Segurança da Informação em conjunto com a área de Tecnologia da Informação do órgão ou entidade;

5.1.2 conduzir auditorias, elaborar relatórios com os resultados e apresentar recomendações de ações preventivas e corretivas.

5.2 **Áreas de Negócio do Órgão ou Entidade**:

5.2.1 elaborar e implementar planos de ação para prevenção e correção de não conformidades observadas durante o processo de auditoria.

5.3 **Área de Tecnologia da Informação do Órgão ou Entidade**:

5.3.1 identificar necessidades de Auditoria da Segurança da Informação;

5.3.2 prover os recursos necessários para a execução da auditoria;

5.3.3 garantir a segurança dos dados gerados pelo processo de auditoria;

5.3.4 apoiar a implementação dos planos de ação relativos à auditoria, gerados pelas áreas de negócio;

5.3.5 conduzir análises críticas com vistas ao aprimoramento da Política de Segurança da Informação do órgão ou entidade da Administração Pública do Poder Executivo Estadual.

6. Documentos Relacionados

- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.
- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.

7. Data de Revisão

- 23/11/2015

Norma 08 - Gestão de Continuidade de Negócios

1. Objetivo

Estabelecer, no âmbito da Administração Pública do Poder Executivo Estadual, as regras e os princípios que regulamentam a Gestão da Continuidade do Negócio – GCN, que são: manter o negócio em funcionamento, definir o papel de cada elemento que administrará a situação da GCN e conscientizar todos os usuários sobre suas responsabilidades no processo.

2. Definições

Continuidade do Negócio: capacidade estratégica e tática do órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios para conseguir continuar suas operações em um nível aceitável e previamente definido.

Gestão de Continuidade de Negócios: processo de gestão que identifica ameaças em potencial e os possíveis impactos às operações de negócio caso essas ameaças se concretizem. Este processo fornece um *framework* para que se construa uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar a reputação e a marca do órgão ou entidade e suas atividades de valor agregado.

Partes Interessadas: aqueles que possuem um interesse permanente nos resultados de uma organização.

Plano de Continuidade de Negócios (PCN): conjunto de procedimentos e planos que visa garantir a continuidade das operações normais da organização, mesmo após ocorrência de um desastre ou indisponibilidade de recursos que sustentam os processos de negócio.

Resiliência Organizacional: capacidade do órgão ou entidade de reagir a um incidente de Segurança da Informação que provoque a interrupção das operações críticas, a tempo de reduzir ou eliminar os danos desta interrupção, incluindo a capacidade estratégica e tática para planejar e responder a incidentes e interrupções do negócio com a finalidade de continuar as operações do negócio a um nível pré-definido e aceitável.

Sistema de Gestão de Continuidade de Negócios (SGCN): parte do sistema global de gestão que estabelece, implementa, opera, monitora, analisa criticamente, mantém e melhora a continuidade de negócios.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os usuários e processos da Administração Pública do Poder Executivo Estadual, bem como, aos sistemas informatizados e meios convencionais de processamento, comunicação e armazenamento de informações.

4. Diretrizes

4.1 A Gestão da Continuidade de Negócio (GCN) na Administração Pública do Poder Executivo Estadual deve:

4.1.1 sistematizar o entendimento integral de todos os aspectos e fenômenos relacionados à Continuidade do Negócio, incluindo:

a) identificação das ameaças potenciais e os respectivos impactos nas operações do negócio do órgão ou entidade;

b) definição da estratégia de recuperação a ser utilizada caso ocorra um incidente;

c) gerenciamento de incidente adverso que interrompa um processo ou atividade crítica;

d) planejamento da continuidade e da recuperação das operações e sistemas após uma interrupção;

e) estabelecimento de procedimentos de retorno à normalidade, quando aplicável;

f) o desenvolvimento de novos produtos e serviços críticos dos órgãos e entidades, assim como mudanças nos existentes, devem ser seguidos por atualizações no PCN para que suas estratégias e ações continuem válidas;

g) estabelecer um programa efetivo para planejamento, resposta a incidentes e à interrupções nos processos de negócio;

h) prover a continuidade das operações do negócio em um nível aceitável;

i) aumentar o poder de recuperação da organização contra o rompimento ou interrupção de sua habilidade de fornecer seus produtos e serviços;

j) orientar ações de prevenção e mitigação dos riscos operacionais;

k) prover a organização de uma metodologia para a elaboração do PCN que possibilite o restabelecimento da sua habilidade de fornecer seus produtos e serviços críticos;

l) desenvolver e implementar um Sistema de Gestão de Continuidade de Negócios para os órgãos ou entidades, que deve ser aceito e seguido inclusive pelas empresas prestadoras de serviço;

m) estabelecer um programa de treinamento e conscientização dos usuários.

5. Competências

5.1 **Alta Administração do Órgão ou Entidade**:

5.2.1 prover apoio estratégico à Gestão da Continuidade de Negócio.

5.2 **Gestores das Áreas de Negócio do Órgão ou Entidade**:

5.3.1 viabilizar, atualizar, manter e implementar os Planos de Continuidade de Negócios.

5.3 **Usuários**:

5.4.1 conhecer os planos existentes e as situações em que serão utilizados, além dos procedimentos em que sua participação esteja prevista.

6. Documentos Relacionados

- ABNT NBR ISO/IEC 27001:2013- Tecnologia da Informação - Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação - Requisitos.
- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação.
- ISO/IEC Guide 73:2009 - Gestão de riscos - Vocabulário.
- Sistemas de Gestão da Continuidade do Negócio – BS/ISO 22313:2012 - *Societal security. Business continuity management systems. Guidance*.
- Normas de Controle de TI, Cobit – *Control Objectives for Information and related Technology.*
- ABNT NBR15999-1:2007 - Versão corrigida 2008 - Gestão de Continuidade de Negócios - Parte 1: Código de prática.
- ABNT NBR ISO/IEC 22301:2013 – Segurança da Sociedade – Sistema de Gestão de Continuidade de Negócios - Requisitos.
- ABNT NBR ISO/IEC 27005:2011 - Tecnologia da Informação - Técnicas de segurança - Gestão de Riscos de Segurança da Informação.
- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.

7. Data de Revisão

- 23/11/2015.

Norma 09–Gestão de Riscos

1. Objetivo

Estabelecer as diretrizes do processo de Gestão de Riscos no âmbito da Segurança da Informação para a Administração Pública do Poder Executivo Estadual.

2. Definições

Alta Administração: dirigente máximo dos órgãos e entidades da Administração Pública do Poder Executivo Estadual, chefes de gabinete, superintendentes e diretores. A Alta Administração dos órgãos e entidades também pode ser proprietária, custodiante ou usuária da informação.

Análise de Riscos: processo de compreender a natureza do risco e determinar o seu nível.

Avaliação de Riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

Controle: qualquer processo, política, dispositivo, prática ou outras ações que modifiquem o risco, podendo ser de natureza administrativa, técnica, de gestão ou legal.

Risco: combinação de consequências de um evento e a probabilidade de ocorrência associada.

Risco Residual: risco remanescente após o seu tratamento.

Tratamento de Riscos: processo de seleção e implementação de medidas para modificar riscos.

3. Abrangência

Esta Norma se aplica a todos os processos críticos de negócio da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Deve ser estabelecida uma metodologia para Gestão de Riscos, contemplando a definição do contexto, análise e avaliação, tratamento, aceitação e comunicação de riscos.

4.2 A Gestão de Riscos deve ser um processo contínuo, através de constante monitoramento e análise crítica dos riscos para os processos de negócio.

4.3 Deve ser definido um período para o ciclo de análises de risco.

4.4 Análises críticas devem ser conduzidas com o objetivo de melhoria do próprio processo de gerenciamento de riscos.

4.5 Definição do Contexto de Riscos:

4.5.1 Deve ser definido um contexto para toda análise de riscos, contemplando, entre outros:

a) objetivos estratégicos da Administração Pública do Poder Executivo Estadual;

b) formalização do escopo da análise de riscos;

c) avaliação de requisitos de Segurança da Informação;

d) incidentes de Segurança da Informação;

e) política de Segurança da Informação;

f) resultados de análises de riscos anteriores;

g) monitoração do ambiente externo, identificando ameaças, riscos e vulnerabilidades.

4.6 Análise de Riscos

4.6.1 Uma análise dos relacionamentos existentes entre os processos de negócio, seus sistemas e serviços, e, respectivos ativos, deve ser conduzida em sintonia com o contexto definido, para estabelecer as prioridades da análise de riscos.

4.6.2 As análises de riscos devem ser executadas como projetos. Cada projeto deve ter a ciência da Alta Administração do órgão ou entidade e um responsável definido.

4.6.3 As análises de riscos devem ser planejadas, contemplando uma avaliação do escopo da análise, definição de cronograma, estratégia de comunicação e estimativa de custos, quando aplicável.

4.6.4 As análises de riscos devem gerar relatórios operacionais e executivos com o objetivo de auxiliar a fase de avaliação de riscos.

4.7 Avaliação de Riscos

4.7.1 Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

4.7.2 Com base nos critérios de risco estabelecidos, os riscos aceitáveis devem ser aceitos formalmente pela Alta Administração e os riscos não aceitáveis devem ser tratados.

4.8 Tratamento e Comunicação de Riscos

4.8.1 O tratamento de riscos deve ser planejado, através da definição:

a) dos controles a serem implementados e de seus responsáveis;

b) da identificação de premissas e restrições, quando aplicáveis;

c) da definição de um cronograma de implementação.

4.8.2 Antes da implementação de qualquer controle, deverá ser feita uma análise de impacto no ambiente que sofrerá a mudança.

4.8.3 Todos os controles não implementados devem ser formalmente documentados e justificados.

4.8.4 Ao final da fase de tratamento, relatórios devem ser elaborados contemplando:

a) o escopo das implementações;

b) a equipe envolvida no processo;

c) os controles implementados;

d) os índices de risco e conformidade pré e pós implementações;

e) os riscos residuais.

4.9 O resultado das Análises e Avaliações de Risco de Segurança da Informação deve ser classificado como informação sigilosa, quando esse puder comprometer a segurança dos processos de negócio do órgão ou entidade a que se refere.

5. Competências

5.1 Alta Administração do Órgão ou Entidade:

5.1.1 autorizar e viabilizar o processo de gestão de riscos;

5.1.2 estabelecer e formalizar os critérios de aceitação dos riscos e os objetivos dos índices de risco e de conformidade.

5.2 **Áreas de Negócio do Órgão ou Entidade**:

5.2.1 em conjunto com a área de Tecnologia da Informação, analisar os resultados provenientes das análises de riscos executadas nos ativos sob sua responsabilidade, definindo planos de ação para aplicação dos controles recomendados, quando aplicável;

5.2.2 aceitar ou tratar os riscos conforme os critérios estabelecidos pela Alta Administração do órgão ou entidade.

5.3 **Área de Tecnologia da Informação do Órgão ou Entidade**:

5.3.1 viabilizar a implementação dos controles sob sua competência;

5.3.2 estabelecer o contexto de riscos em conjunto com as áreas envolvidas;

5.3.3 executar periodicamente os processos de análise, avaliação, comunicação e tratamento de riscos.

6. Documentos Relacionados

- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual.
- ABNT NBR ISO 31000:2009 - Gestão de Riscos - Princípios e diretrizes.
- ABNT NBR ISO/IEC 27005:2011– Tecnologia da Informação – Técnicas de Segurança - Gestão de Riscos de Segurança da Informação.

7. Data de Revisão

- 23/11/2015

Norma 10 - Contabilização de Ativos de Tecnologia da Informação

1. Objetivo

Definir as diretrizes para a contabilização adequada dos Ativos de Tecnologia da Informação no âmbito da Administração Pública do Poder Executivo Estadual.

2. Definições

Ativos de Tecnologia da Informação: estações de trabalho, servidores, *softwares*, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como processos, pessoas e ambientes.

Estação de Trabalho: todos os computadores e equipamentos correlatos da Administração Pública do Poder Executivo Estadual, inclusive dispositivos móveis.

Freeware: programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso.

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Mídias Removíveis/Reutilizáveis: incluem fitas, discos, memórias *flash*, discos removíveis, CD, DVD, mídia impressa, entre outros.

Shareware: programa disponível publicamente para avaliação e uso experimental, mas, cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. *Shareware* é distinto de *freeware*, no sentido de que um *software shareware* é comercial, embora em termos e preços diferenciados em relação a um produto comercial convencional.

***Software* Livre**: denominação dada a determinado *software* cujo código-fonte é de domínio público e, em geral, gratuito.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os usuários dos Ativos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 As informações e os Ativos de Tecnologia da Informação de propriedade da Administração Pública do Poder Executivo Estadual devem ser utilizados

exclusivamente para os seus interesses, podendo ser monitorados a qualquer tempo.

4.2 Os Ativos de Tecnologia da Informação devem ser inventariados e identificados de forma única.

4.3 Os Ativos de Tecnologia da Informação devem ser classificados em função de sua relevância para o processo de negócio a que se destinam. Esta relevância deve ser considerada em eventuais análises de riscos.

4.4 Os Ativos de Tecnologia da Informação devem ser, sempre que possível, relacionados a um usuário, responsável por sua utilização.

4.5 A entrada e a saída de Ativos de Tecnologia da Informação das dependências dos órgãos e entidades da Administração Pública do Poder Executivo Estadual devem ser acompanhadas pelos devidos documentos de movimentação.

4.6 O padrão de configuração (*hardware e software*) dos Ativos de Tecnologia da Informação é definido pela área de Tecnologia da Informação dos órgãos e entidades e não deve ser modificado sem sua autorização.

4.7 Os itens que compõem conjuntos de ativos não podem ser modificados sem a autorização da área de Tecnologia da Informação dos órgãos e entidades.

4.8 Somente *softwares* licenciados e homologados devem ser utilizados.

4.9 Os inventários (*hardware e software*) devem ser atualizados apropriadamente sempre que Ativos de Tecnologia da Informação sofrerem mudanças.

4.10 As mídias contendo as cópias de segurança devem ser catalogadas e armazenadas por tempo compatível com as necessidades dos processos de negócio.

4.11 A utilização de *software* que não seja de propriedade da Administração Pública do Poder Executivo Estadual ou licenciado para a mesma, pode, além de configurar crime de pirataria conforme Lei Nº 9.609, de 19 de fevereiro de 1998, interferir na contabilização dos ativos.

5. Competências

5.1 **Área de Tecnologia da Informação do Órgão ou Entidade**:

5.1.1 contabilizar os Ativos de Tecnologia da Informação de forma a garantir sua conformidade com esta Norma.

5.2 **Usuário**:

5.2.1 utilizar os Ativos de Tecnologia da Informação em conformidade com esta Norma;

5.2.2 notificar, através de abertura de incidente de Segurança da Informação, sempre que identificar dano, roubo, perda ou modificações indevidas em um Ativo de Tecnologia da Informação.

6. Documentos Relacionados

- Norma 04 - Acesso aos Recursos de Tecnologia da Informação.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

7. Data de Revisão

- 23/11/2015

Norma 11 - Intercâmbio de Informações

1. Objetivo

Definir as diretrizes de segurança na troca de informações e *softwares* internamente, entre os órgãos e entidades da Administração Pública do Poder Executivo Estadual e/ou com quaisquer entidades externas.

2. Definições

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Mídias Removíveis/Reutilizáveis: incluem fitas, discos, memórias *flash*, discos removíveis, CD, DVD, mídia impressa, entre outros.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

***Virtual Private Network* (VPN)**: rede virtual privada com uso de criptografia para garantir a confidencialidade das informações trafegadas em uma rede pública.

3. Abrangência

Esta Norma se aplica a todos os usuários de informações ou sistemas de informação de propriedade da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Diretrizes Gerais

4.1.1 A troca de informações entre os usuários deve ser suportada por acordos formalizados e documentados, contendo, quando aplicável, cláusulas de preservação da privacidade de dados pessoais, direitos autorais, preservação de bens patrimoniais, sigilo e não divulgação.

4.1.2 Salvo nos casos previstos em lei, todo usuário deve assinar um termo de sigilo e confidencialidade com o Governo do Estado da Bahia.

4.1.3 As informações classificadas como sigilosas gravadas em mídia removível devem utilizar solução de criptografia.

4.1.4 Toda informação sigilosa deve receber o tratamento adequado conforme descrito na Norma de Classificação da Informação.

4.1.5 Procedimentos de recepção de *fac-símiles*, impressão de documentos, abertura de correio e distribuição de correspondência devem ser estabelecidos de forma a prevenir o acesso não autorizado à informação.

4.1.6 Ações de conscientização dos usuários devem incluir a observância das necessidades de segurança ao se efetuar conversações, inclusive as telefônicas, sobre assuntos restritos e confidenciais em locais públicos, em escritórios abertos ou mesmo em reuniões realizadas em sala sem a devida adoção dos requisitos de segurança.

4.1.7 Mecanismos devem ser implementados para proteger as informações associadas aos sistemas de informação dos negócios, entre outros:

a) proteção contra interceptação e gravação de chamadas telefônicas ou de teleconferências, garantindo a confidencialidade das chamadas;

b) o acesso à rede corporativa ou a *Intranet*, por meio da *Internet*, deve utilizar solução de criptografia, a exemplo de VPN (*Virtual Private Network)*;

c) procedimento de retenção de cópias de segurança das informações mantidas nos sistemas, bem como sua recuperação e contingência;

d) restrição de acesso a informações de trabalho compatível às atividades do usuário através do gerenciamento de perfis de acesso;

e) proteção contra código malicioso, conforme Norma de Proteção Contra Código Malicioso;

f) procedimentos para o uso de comunicação sem fio, levando em conta os riscos particulares envolvidos;

g) as mensagens confidenciais, enviadas pelo Correio Eletrônico, devem utilizar solução de criptografia.

4.2 Mídias em Trânsito

4.2.1 Devem ser adotados transporte e serviço de mensageiro confiável e preferencialmente estabelecer um contrato de sigilo e confidencialidade com esse serviço.

4.2.2 As embalagens de mídias removíveis devem ser suficientes para proteger os conteúdos contra danos físicos.

4.2.3 Mecanismos de proteção contra danos físicos durante o transporte das mídias removíveis devem ser adotados, considerando as recomendações do fabricante das mídias.

4.2.4 A entrega dos documentos e das mídias removíveis, contendo informações sigilosas, deve ser registrada em recibo ou sistema eletrônico específico.

5. Competências

5.1 **Área de Tecnologia da Informação do Órgão ou Entidade**:

5.1.1 prover recursos para garantir a troca adequada de *software*, de informações armazenadas e transmitidas por meio eletrônico.

5.2 **Usuário**:

5.2.1 cumprir as diretrizes desta norma.

6. Documentos Relacionados

- Norma 02 - Classificação da Informação.
- Norma 05 - Acesso e Utilização do Correio Eletrônico.
- Norma 16 - Proteção Contra Código Malicioso.

7. Data de Revisão

- 23/11/2015

Norma 12 - Segurança Física

1. Objetivo

Estabelecer diretrizes para prevenir o acesso físico não autorizado, a fim de evitar danos e interferência às informações, ativos e instalações físicas da Administração Pública do Poder Executivo Estadual.

2. Definições

Área Protegida: corresponde às dependências dos órgãos e entidades, onde escritórios, salas e instalações de processamento de informações são utilizados pela Administração Pública do Poder Executivo Estadual.

Área Pública: corresponde ao perímetro externo às dependências dos órgãos e entidades, tais como ruas, avenidas e áreas circunvizinhas e instalações prediais, quando as dependências do órgão ou entidade estão em salas ou andares de prédios comerciais.

Área Segura: incluem-se nesta classificação especial as áreas protegidas que contenham informações, dispositivos ou serviços imprescindíveis aos negócios, tais como sala de servidores, sala de operação, cofre, salas e armários com informações sensíveis associadas a interesses relevantes dos órgãos e entidades e locais com equipamentos e infraestrutura de conectividade (*switches,* roteadores, dispositivos de armazenamento, quadro de telefonia, quadro de cabeamento, entre outros).

3. Abrangência

Esta Norma se aplica a todas as dependências e usuários da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Perímetros de Segurança

4.1.1 Em Áreas Públicas:

a) as regras de controle de acesso físico não se aplicam às áreas públicas.

4.1.2 Em Áreas Protegidas:

a) devem ser localizados de forma a evitar o acesso do público, com indicações mínimas do seu propósito e sem sinais óbvios da presença de atividades de processamento de informação;

b) convém que as paredes externas possuam construção sólida. As portas externas devem ser protegidas de forma apropriada, com mecanismos de controle, travas etc., contra acessos não autorizados; uma área de recepção ou outro meio de controle de acesso físico deve ser usado, devendo o acesso ser restrito apenas ao pessoal autorizado;

c) barreiras físicas devem, se necessário, ser estendidas da laje do piso até a laje superior para prevenir acessos não autorizados ou contaminação ambiental como as causadas por fogo e inundações;

d) todas as portas de incêndio devem possuir dispositivo para fechamento automático;

e) devem ser afixados avisos (normalmente nas entradas, saídas e corredores de acesso), facilmente visíveis, informando sobre o controle de acesso para as pessoas e alertando sobre as restrições ao acesso público, de tal forma que desestimule as invasões.

4.1.3 Em Áreas Seguras:

a) barreiras e perímetros adicionais para controlar o acesso físico podem ser necessários em áreas com diferentes requisitos de segurança dentro de um mesmo perímetro de segurança;

b) devem ser afixados avisos, normalmente na respectiva porta, facilmente visíveis, alertando sobre as restrições ao acesso às áreas seguras, indicando que somente pessoal autorizado tem acesso, de tal forma que desestimule as invasões.

4.2 Controles de Entrada Física

4.2.1 Procedimentos de controle de acesso físico devem ser implementados de forma a restringir o acesso às áreas protegidas e seguras. Os procedimentos de controle de acesso devem, quando necessário, contemplar, entre outros:

a) a utilização de dispositivos de identificação pessoal;

b) monitoração de acessos;

c) restrições de horários de acesso e permanência;

d) controle de acesso de terceiros;

e) movimentação de ativos.

4.2.2 O pessoal autorizado deve ter acesso físico somente aos ativos imprescindíveis para a realização dos seus trabalhos.

4.2.3 O acesso de visitantes deve se dar somente após identificação individual e autorização de entrada por parte da pessoa e/ou setor que será visitado.

4.3 Segurança em Escritórios, Salas e Instalações de Processamento

4.3.1 A escolha da localização, os projetos de engenharia e arquitetura das instalações devem levar em consideração as possibilidades de danos causados por fogo, inundações, explosões, manifestações civis e outras formas de desastres naturais ou causados pelo homem. Também devem ser levados em consideração as regulamentações e padrões de segurança e saúde, bem como serem tratadas quaisquer ameaças originadas em propriedades vizinhas.

4.3.2 Portas e janelas devem ser mantidas fechadas quando não utilizadas e devem ser instaladas proteções extras, principalmente quando essas portas e janelas se localizarem em andar térreo.

4.3.3 Sistemas de detecção de intrusos, tais como alarmes e sistemas de vídeo vigilância, devem ser instalados e testados regularmente, de forma a cobrir todas as portas e janelas acessíveis.

4.3.4 Equipamentos de contingência e meios magnéticos de reserva devem ser guardados a uma distância segura para evitar danos que podem se originar de um desastre na área protegida.

4.3.5 As portas de entrada devem permanecer trancadas nos períodos de inatividade.

4.3.6 Uma "política de mesa limpa" deve ser implementada, visando eliminar riscos de acesso não autorizado a informações em mídias não magnéticas, tais como documentos sensíveis deixados em impressoras ou mesas de trabalho.

4.4 Trabalho em Áreas Seguras

4.4.1 A existência das informações ou das atividades dentro de áreas seguras deve ser de conhecimento restrito a pessoal autorizado e apenas quando necessário.

4.4.2 Áreas seguras devem estar fechadas e trancadas adequadamente de forma a impedir acessos não autorizados. Quando desocupadas, devem ser mantidas fisicamente fechadas e verificadas periodicamente.

4.4.3 Somente pessoas imprescindíveis à realização dos trabalhos rotineiros ou de manutenção devem ter acesso às áreas seguras, mediante autorização.

4.4.4 Deve-se evitar trabalho sem monitoramento nas áreas seguras para prevenir oportunidades de atividades maliciosas, devendo o pessoal de serviços de suporte terceirizado ter acesso controlado a estas áreas.

4.4.5 Materiais combustíveis ou perigosos devem ser guardados de forma adequada a uma distância apropriada de uma área segura. Suprimentos volumosos, tais como material de escritório, não devem ser guardados em áreas seguras, a menos que sejam imprescindíveis.

4.4.6 Qualquer equipamento de gravação, fotográfico, vídeo ou som somente deve ser utilizado com autorização.

4.5 Instalação e Proteção dos Equipamentos

4.5.1 Os Ativos de Tecnologia da Informação devem ser posicionados fisicamente e protegidos, a fim de se reduzir o risco decorrente de ameaças potenciais e oportunidades de acesso não autorizado.

4.5.2 O consumo de alimentos, bebidas e fumo deve acontecer apenas nas instalações definidas para esse fim.

4.5.3 Os Ativos de Tecnologia da Informação críticos devem ser protegidos por equipamentos contra falhas de energia e outras anomalias na alimentação elétrica.

4.5.4 As áreas consideradas pela Administração Pública do Poder Executivo Estadual como sendo de alto risco devem possuir planos de continuidade operacional que estabeleçam as atividades necessárias para contingência e restauração dos Ativos de Tecnologia da Informação, de forma a garantir a disponibilidade dos serviços, mesmo em momentos de crise.

4.5.5 Normas Técnicas Brasileiras devem ser seguidas no que concerne ao cabeamento de redes, telecomunicações e instalações elétricas.

4.5.6 O cabeamento de dados e as instalações elétricas devem ser protegidos contra interceptação ou dano.

4.5.7 Os pontos de rede de dados devem ser controlados, devendo-se documentar todos os pontos existentes e evitar a existência de pontos ativos sem utilização.

5. Competências

5.1 **Área de Tecnologia da Informação do Órgão ou Entidade**:

5.1.1 garantir que os Ativos de Tecnologia da Informação estejam fisicamente protegidos contra ameaças à sua segurança, conforme as diretrizes desta Norma;

5.1.2 realizar auditorias periódicas visando o cumprimento das diretrizes desta Norma;

5.1.3 tratar os incidentes de segurança abertos em função de não conformidades observadas.

5.2 **Usuário**:

5.2.1 observar e cumprir todas as diretrizes desta Norma;

5.2.2 reportar quaisquer não conformidades através de abertura de incidente de segurança.

6. Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013– Tecnologia da Informação –Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

7. Data de Revisão

- 23/11/2015

Norma 13 - Segurança em Terceirização e Prestação de Serviços

1. Objetivo

Estabelecer diretrizes para implementar e manter o nível apropriado de Segurança da Informação e de entrega de serviços nos acordos firmados entre o Governo do Estado da Bahia e terceiros.

2. Definições

Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio.

Parceiro: qualquer entidade pública ou privada, organizações não governamentais ou instituições sem fins lucrativos com a qual se estabeleça uma relação de cooperação mútua.

Terceiro: qualquer parceiro, fornecedor ou prestador de serviço que acesse informações ou utilize recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual.

3. Abrangência

Esta Norma se aplica a todos os acordos celebrados entre o Governo do Estado da Bahia e terceiros.

4. Diretrizes

4.1 *Contratos* firmados entre o Governo do Estado e prestadores de serviço devem incluir acordos que definam os níveis de entrega de serviços, contemplando, entre outros:

4.1.1 definição explícita das responsabilidades e direitos legais do Governo do Estado, da Prestadora de Serviços e dos profissionais envolvidos;

4.1.2 definição explícita dos direitos de propriedade dos produtos gerados;

4.1.3 aceite obrigatório de toda a Política de Segurança da Informação do contratante;

4.1.4 acordos de confidencialidade entre ambas as partes;

4.1.5 acordos de confidencialidade entre o terceiro e seus funcionários e subcontratados;

4.1.6 limitação do acesso apenas aos ativos e informações necessários à execução de suas atividades;

4.1.7 cláusulas contratuais que garantam a continuidade operacional durante os períodos de transição;

4.1.8 nível de capacidade técnica, logística e administrativa necessária do terceiro para prestar os serviços contratados;

4.1.9 planos para garantir os níveis de continuidade de serviços acordados após falhas severas nos serviços ou desastres;

4.1.10 acordos de nível de serviço (SLA), com indicadores adequados à natureza do contrato;

4.1.11 informação de que os serviços prestados poderão ser auditados.

4.2 Os serviços de terceiros, prestados ao Governo do Estado devem ser monitorados e analisados criticamente de forma regular, a fim de garantir a aderência entre os termos de Segurança da Informação e as condições dos acordos, além de permitir o gerenciamento adequado de problemas e Incidentes de Segurança da Informação.

4.3 Devem ser executadas auditorias periódicas nos serviços de terceiros, contemplando, mas não limitando-se a:

4.3.1 níveis de desempenho de serviço para verificar aderência aos acordos;

4.3.2 relatórios de serviços produzidos por terceiros;

4.3.3 registros dos incidentes de Segurança da Informação e de sua respectiva análise crítica, tanto pelo terceiro quanto pelo órgão ou entidade, como requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiam;

4.3.4 trilhas de auditoria do terceiro e registros de eventos de segurança, problemas operacionais, falhas, investigação de falhas e interrupção relativas ao serviço.

4.4 Um processo de gerenciamento de mudanças deve ser elaborado para os serviços prestados por terceiros a fim de garantir que modificações em recursos de Tecnologia da Informação sejam processadas, levando-se em consideração o grau de importância dos sistemas e processos de negócio envolvidos. Este processo deve contemplar, mas não limitando-se a:

4.4.1 melhoria dos serviços correntemente oferecidos;

4.4.2 desenvolvimento de quaisquer novas aplicações ou sistemas;

4.4.3 modificações ou atualizações das políticas e procedimentos;

4.4.4 novos controles para resolver os incidentes de Segurança da Informação e melhoria da segurança;

4.4.5 mudanças e melhorias em redes;

4.4.6 uso de novas tecnologias;

4.4.7 adoção de novos produtos ou novas versões;

4.4.8 novas ferramentas e ambientes de desenvolvimento;

4.4.9 mudanças de localização física dos recursos de serviços;

4.4.10 mudanças de fornecedores;

4.4.11 mudanças de contratos.

5 Competências

5.1 **Áreas de Negócio do Órgão ou Entidade**:

5.1.1 administrar os contratos sob sua responsabilidade;

5.1.2 monitorar e aprovar periodicamente as atividades dos prestadores de serviços, quanto à qualidade e eficiência;

5.1.3 avaliar regularmente o direito de acesso dos prestadores de serviço sob sua responsabilidade;

5.1.4 comunicar, área de Tecnologia da Informação, infrações aos acordos de segurança estabelecidos por meio de incidentes de Segurança da Informação;

5.1.5 auditar periodicamente os serviços de terceiros.

5.2 **Área de Tecnologia da Informação do Órgão ou Entidade**:

5.2.1 definir, junto as áreas envolvidas, os níveis de entrega de serviços adequados e os requisitos necessários para garantia da segurança das informações;

5.2.2 implementar um processo de gerenciamento de mudanças em recursos de Tecnologia da Informação para serviços de terceiros.

6 Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013–Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- Norma 02 - Classificação da Informação.
- Norma 12 - Segurança Física.
- Norma 11 - Intercâmbio de Informações.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

7 Data de Revisão

- 23/11/2015

Norma 14 - Desenvolvimento e Manutenção de Aplicações

1. Objetivo

Estabelecer as diretrizes que regulamentam a segurança para o processo de desenvolvimento e manutenção de *software* no âmbito da Administração Pública do Poder Executivo Estadual.

2. Definições

Artefato de *Software*: item criado como parte da definição, manutenção ou utilização de um processo de *software*, incluindo, entre outros, descrições de processos, planos, procedimentos, especificações, projetos de arquitetura, projeto detalhado, código, documentação para o usuário.

Base de Dados: conjunto de dados organizados de forma a servir de base para que o usuário processe e recupere informações.

Gestão de Configuração: conjunto de procedimentos técnicos e gerenciais que são definidos para identificação de Ativos de Tecnologia da Informação e para a gestão de suas alterações.

Rastreabilidade: capacidade de acompanhamento e registro de todos os eventos e movimentações ocorridas, desde a criação da informação até o seu descarte.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os usuários envolvidos nos processos de desenvolvimento e manutenção de *software* no âmbito da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Disposições Gerais

4.1.1 Pelo menos 1 (uma) metodologia deve ser estabelecida para todo desenvolvimento ou manutenção, com base nas melhores práticas de mercado, contemplando, entre outros:

a) planejamento;

b) análise de requisito;

c) projeto;

d) codificação;

e) revisão;

f) compilação;

g) teste.

4.1.2 Todo desenvolvimento ou manutenção de *software* deve ser formalmente autorizado.

4.1.3 Para todo desenvolvimento ou manutenção de *software* deve ser realizada uma análise de impacto.

4.1.4 Toda alteração de escopo de desenvolvimento ou manutenção de *software* deve ser documentada e formalmente autorizada.

4.1.5 Todas as ferramentas de desenvolvimento devem ser homologadas e licenciadas.

4.1.6 Todo projeto de *software* deve conter um documento de especificação que descreva seus requisitos de segurança, os quais devem, entre outros, contemplar:

a) mecanismo de autenticação do usuário, que deve utilizar senhas com métrica mínima e exigir do usuário a troca periódica da senha;

b) o mecanismo de autenticação do usuário, que deve bloquear o acesso após número definido de tentativas de *login* com falha;

c) a verificação da senha por meio de mecanismo que impeça fraudes de repetição, interceptação ou quebra de integridade na comunicação entre o cliente e o servidor;

d) a escolha da senha por novos usuários sem a interferência do pessoal de apoio ou o recebimento pelos mesmos, de uma senha inicial que precise ser trocada;

e) o armazenamento da senha pelo sistema, de forma criptografada e irreversível;

f) a uniformidade do controle de acesso em todo o sistema, utilizando-se uma única rotina de verificação;

g) a realização do controle de acesso na camada mais próxima possível dos dados;

h) o registro, pelo sistema, dos eventos significativos para a segurança, principalmente, início e fim do mecanismo de auditoria;

i) o registro, pelo sistema, das falhas de *login*, indicando o número de tentativas;

j) o registro, pelo sistema, da criação e remoção de usuários, bem como da atribuição e da remoção de direitos do usuário;

k) a proteção da trilha de auditoria contra remoção e alteração por parte de todos os usuários, exceto dos administradores de auditoria;

l) a capacidade de tolerância do sistema à falhas e retorno a operação;

m) a inexistência, em aplicações web, de dados sensíveis em campos ocultos ou *cookies*;

n) a realização das verificações e validações de segurança no servidor, em aplicações web;

o) o acesso aos desenvolvedores apenas aos códigos fontes necessários para a alteração, quando autorizados pelo superior imediato;

p) a maior semelhança possível do ambiente de homologação ao ambiente de produção;

q) a exigência de que os aplicativos só passem do desenvolvimento para a homologação após verificação da existência e adequação de sua documentação;

r) a existência de documentação de instalação, configuração e operação do sistema, ressaltando os aspectos de segurança, que deve ser mantida atualizada. Requisitos funcionais, não funcionais e de domínio devem ser especificados e documentados, bem como as manutenções necessárias, considerando os requisitos de segurança definidos no desenvolvimento do sistema.

4.1.7 A especificação dos requisitos deve ser elaborada em conjunto com a área de negócio solicitante da demanda.

4.1.8 Um mecanismo de controle de versão deve ser implementado durante o processo de desenvolvimento e manutenção de *software*.

4.1.9 Deve existir um programa de conscientização em Segurança da Informação para todos os usuários envolvidos nos processos de desenvolvimento de aplicações.

4.1.10 Devem existir mecanismos de verificação de vulnerabilidades no código fonte durante o processo de desenvolvimento e manutenção de *software*.

4.1.11 Incidentes de segurança devem ser abertos quando vulnerabilidades forem identificadas durante o processo de desenvolvimento e manutenção de *software*.

4.1.12 O acesso aos códigos fontes deve ser controlado e restrito aos desenvolvedores envolvidos, em seus respectivos projetos.

4.1.13 Os códigos fontes não devem conter identificações e/ou senhas de acesso às bases de dados, sejam elas de teste, de homologação ou de produção.

4.1.14 Ambientes de desenvolvimento e testes, de homologação e de produção devem ser isolados entre si.

4.1.15 Um processo de gestão de configuração deve ser implementado e deve abranger todo o processo de desenvolvimento e manutenção.

4.2 Todo *software* que implique em manipulação de dados deve ser desenvolvido com controle de acesso lógico. Mecanismos adicionais que possibilitem a rastreabilidade das operações efetuadas devem ser considerados em casos de manipulação de dados sensíveis.

4.3 Desenvolvimento Terceirizado

4.3.1 Todos os contratos com terceiros devem contemplar cláusulas de sigilo e confidencialidade.

4.3.2 Os produtos desenvolvidos externamente devem obedecer a padrões e metodologias homologadas, além de atender aos requisitos funcionais, não funcionais, de domínio e de segurança definidos.

4.3.3 O contrato de desenvolvimento de produtos com terceiros deve prever, no mínimo, os artefatos de *software* a serem entregues em cada fase, a validação, o procedimento de aceite final e o período de garantia.

4.4 Testes

4.4.1 Procedimentos de testes no *software* devem ser definidos e utilizados para todo desenvolvimento ou manutenção realizados, e devem contemplar, entre outros, controles tais como:

a) validação de dados de entrada;

b) controle de processamento interno;

c) integridade de mensagens;

d) validação de dados de saída.

4.4.2 Os testes devem validar os mecanismos de segurança especificados no desenvolvimento ou na manutenção do *software*.

4.4.3 Os testes de aceitação do *software* devem ser realizados por uma equipe diferente da equipe desenvolvedora, que deve ser composta por usuários da área de desenvolvimento e da área de negócio solicitante.

4.4.4 A utilização de dados de produção em ambiente de testes deve ser autorizada formalmente.

4.4.5 As informações contidas na base de dados de ambiente de produção, se utilizadas para testes, devem sofrer alterações, de modo a preservar sua confidencialidade.

4.5 Aceitação de *Software*

4.5.1 Os artefatos de *software*, provenientes de desenvolvimento ou manutenção, devem ser homologados antes de serem utilizados em ambiente de produção.

4.6 Mudanças Técnicas no Ambiente de Produção

4.6.1 As atualizações de configuração no ambiente de produção devem ser realizadas, inicialmente, em ambiente de teste e, todo *software* deve ser analisado criticamente, considerando os seguintes aspectos:

a) análise crítica dos procedimentos de controle e integridade do *software*, garantindo que os mesmos não foram comprometidos pelas mudanças efetuadas no ambiente de produção;

b) revisão do planejamento e do orçamento anual para suporte, garantindo investimentos para revisões e testes de *softwares* resultantes das modificações do ambiente de produção;

c) revisão do Plano de Continuidade dos Negócios para contemplar mudanças necessárias resultantes das modificações do ambiente de produção.

4.7 Implantação

4.7.1 Os produtos homologados devem ser implantados em ambiente de produção, por meio de procedimentos técnicos definidos pela área de Tecnologia da Informação do órgão ou entidade e aceite da área cliente.

4.7.2 Planos de Continuidade Operacional devem ser desenvolvidos pelas áreas de negócio do órgão ou entidade para garantir a continuidade dos processos envolvidos nas implantações de *software* ou outras mudanças relacionadas.

4.7.3 A implantação de novo *software* deve ser realizada de acordo com o calendário definido pelas áreas de negócio do órgão ou entidade, com a participação da respectiva área de Tecnologia da Informação.

5. Competências

5.1 Áreas de Negócio do Órgão ou Entidade:

5.2.1 autorizar a utilização de dados de produção no ambiente de testes;

5.2.2 elaborar procedimentos de homologação, homologar e dar aceite aos produtos desenvolvidos pela área de Tecnologia da Informação do órgão ou entidade;

5.2.3 elaborar Planos de Continuidade Operacional para garantir a continuidade dos processos envolvidos nas implantações de *software* ou outras mudanças relacionadas.

5.2 Área de Tecnologia da Informação do Órgão ou Entidade:

5.1.1 homologar os procedimentos e metodologias de desenvolvimento externo;

5.1.2 definir treinamentos necessários para os desenvolvedores;

5.1.3 analisar os impactos das solicitações de desenvolvimento e modificações e autorizar ou realizar o desenvolvimento ou a manutenção;

5.1.4 definir procedimentos de testes e implantação de *software*;

5.1.5 realizar testes no *software* desenvolvido ou modificado;

5.1.6 homologar *software* e ferramentas de desenvolvimento de *software*;

5.1.7 disponibilizar ferramenta para atualizar *software* no ambiente de produção.

6. Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013– Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- ISO/IEC 15408-1:2009*Information technology - Security techniques -- Evaluation criteria for IT security-- Part 1: Introduction and general model.*
- ISO/IEC15408-2:2008Information technology - Security techniques -- Evaluation criteria for IT security—Part 2: Security functional components
- ISO/IEC15408-3:2008Information technology - Security techniques -- Evaluation criteria for IT security—Part3: Security assurance components
- Norma 11 - Intercâmbio de Informações.
- Norma 10 - Contabilização de Ativos de Tecnologia da Informação.
- Norma 02 - Classificação da de Informação.

7. Data de Revisão

- 23/11/2015

Norma 15 - Distribuição de Hardware e Software

1. Objetivo

Estabelecer diretrizes para a aquisição, distribuição e gerenciamento de *hardware* e *software* no âmbito da Administração Pública do Poder Executivo Estadual.

2. Definições

Biblioteca de *Software* Definitivo: repositório no qual as versões autorizadas e definitivas de todos os itens de *software* em produção estão armazenadas e protegidas.

Depósito de *Hardware* Definitivo: área separada para o armazenamento de todos os itens definitivos de *hardware* sobressalente.

Freeware: programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso.

Processo de Gestão de Mudanças: processo que assegura que métodos e procedimentos padronizados sejam utilizados para um tratamento rápido e eficiente de todas as mudanças, de modo a minimizar o impacto de quaisquer incidentes relacionados aos recursos de Tecnologia da Informação.

Shareware: programa disponível publicamente para avaliação e uso experimental, mas, cujo uso em regime pressupõe que o usuário pagará uma licença ao autor. *Shareware* é distinto de *freeware*, no sentido de que um *software shareware* é comercial, embora em termos e preços diferenciados em relação a um produto comercial convencional.

***Software* Livre**: denominação dada a determinado *software* cujo código-fonte é de domínio público e, em geral, gratuito.

3. Abrangência

Esta Norma se aplica a todos os usuários, processos de negócio, sistemas, serviços e Ativos de Tecnologia da Informação da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Aquisição de *Hardware* e *Software*

4.1.1 Toda aquisição de *hardware* ou *software* deve ser precedida de um levantamento das necessidades do processo de negócio a que se destinam, tais como: capacidade de processamento, flexibilidade, estrutura de dados, entre outros.

4.1.2 Antes da aquisição de *hardware* ou *software* críticos e, quando possível, havendo concordância do fornecedor, deve ser conduzida uma POC –*Proof of Concept* (Prova de Conceito).

4.1.3 Todos os itens adquiridos devem ser inventariados conforme norma específica (Norma de Contabilização de Ativos de Tecnologia da Informação) e, quando viável, ser apoiado por uma ferramenta de automação.

4.1.4 Períodos de vida útil devem ser definidos para cada tipo de *hardware*, contemplando as necessidades do processo de negócio a que se destina e o retorno de investimento (ROI) durante seu ciclo de vida.

4.1.5 Planos de atualização de *hardware* e *software* devem ser elaborados considerando seu período de vida útil, os requisitos funcionais e técnicos dos processos de negócio e, de acordo com o direcionamento tecnológico da Administração Pública do Poder Executivo Estadual.

4.2 Distribuição de *Hardware* e *Software*

4.2.1 Deve ser estabelecido um processo de gestão de mudanças que contemple todas as atividades de distribuição de *hardware* e *software*, tais como: adição, modificação e remoção, com o objetivo de controlar os riscos de impacto aos processos de negócio (paralisação ou queda de desempenho prolongadas ou não programadas). Este processo deve contemplar, entre outros:

a) planejamento das mudanças em conjunto com as áreas de negócio do órgão ou entidade e outras partes relevantes;

b) documentação de todas as mudanças (requisição de mudança);

c) formalização da aceitação de mudanças;

d) identificação de medidas de reversão ou remediação se a mudança não for bem sucedida;

e) atualização dos inventários de *hardware* e *software*;

f) instalação de um ambiente de testes para a homologação de mudanças críticas antes de aplicá-las em ambiente de produção;

g) análise de impacto à integridade dos dados (modificações em arquivos de dados feitas pelo sistema ou aplicação sem intervenção direta do usuário);

h) proteção à integridade de *hardware* e *software* durante instalação, manejo e transporte;

i) treinamento a usuários e administradores e documentação correspondente.

4.2.2 Deve ser implementada uma biblioteca de *software* definitivo com o objetivo de garantir que somente versões autorizadas estejam sendo utilizadas, devendo conter:

a) versões originais, definitivas e autorizadas de todo *software* e códigos fonte, quando aplicável;

b) repositório para o armazenamento seguro de todas as cópias originais dos *softwares* e suas respectivas licenças e direitos de propriedade;

c) estrito controle de licenças com o objetivo de eliminar os *softwares* não autorizados;

d) informações relativas à suporte técnico, direitos de atualização, entre outras condições contratuais;

e) documentação e manuais relacionados.

4.2.3 O processo de distribuição de *software* deve, quando cabível, ser apoiado por uma ferramenta da automação.

4.2.4 Deve ser implementado um depósito de *hardware* definitivo com o objetivo de proteger equipamentos sobressalentes, que devem ser mantidos no mesmo nível que os seus correspondentes do ambiente de produção e podem ser utilizados por outros sistemas ou para recuperação de incidentes de grande impacto.

4.2.5 O depósito de *hardware* definitivo deve conter os respectivos manuais e demais documentos atualizados para cada equipamento.

5. Competências

5.1 Áreas de Negócio do Órgão ou Entidade:

5.1.1 requerer as mudanças de acordo com os procedimentos definidos no processo de gestão de mudanças.

5.2 Área de Tecnologia da Informação do Órgão ou Entidade:

5.2.1 elaborar e manter os inventários de *hardware* e *software*;

5.2.2 estabelecer os períodos de vida útil de *hardware* e *software*;

5.2.3 elaborar o plano de atualização de *hardware* e *software*;

5.2.4 implementar o processo de gestão de mudanças para apoiar a distribuição de *hardware* e *software*;

5.2.5 avaliar, aprovar e implementar ou negar as requisições de mudança em cooperação com as áreas de negócio envolvidas;

5.2.6 promover a melhoria contínua do processo de gestão de mudanças;

5.2.7 distribuir os itens de *hardware* e *software*;

5.2.8 implementar a biblioteca de *software* definitivo e o depósito de *hardware* definitivo.

6. Documentos Relacionados

- ABNT NBR ISO/IEC 20000-1:2011 - Tecnologia da informação — Gestão de serviços Parte 1: Requisitos do sistema de gestão de serviços

- ABNT NBR ISO/IEC 27002:2013– Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- ABNT NBR ISO 31000:2009 - Gestão de Riscos - Princípios e diretrizes.
- ITIL – *Information Technology Infrastructure Library*.
- Norma 10 - Contabilização de Ativos de Tecnologia da Informação.
- Norma 09 - Gerenciamento de Riscos.
- Norma 14 - Desenvolvimento e Manutenção de Aplicações.

7. Data de Revisão

- 23/11/2015

Norma 16 - Proteção Contra Código Malicioso

1. Objetivos

Estabelecer diretrizes para a proteção dos recursos de Tecnologia da Informação da Administração Pública do Poder Executivo Estadual contra ação de código malicioso, programas impróprios.

2. Definições

Código Malicioso: termo genérico que se refere a todos os tipos de programa especificamente desenvolvidos para executar ações danosas em recursos de Tecnologia da Informação, tais como vírus, cavalo de tróia*, spyware, worms*, entre outros.

Log: arquivo que contém informações sobre eventos de qualquer natureza em um sistema computacional, análise forense para a elucidação de incidentes de segurança, auditoria de processos, cumprimento de exigências legais para a manutenção de registro do histórico de acessos ou eventos e para a resolução de problemas (*debugging*).

Programas Impróprios: programas utilitários utilizados para explorar vulnerabilidades ou burlar a segurança dos recursos de Tecnologia da Informação.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

3. Abrangência

Esta Norma se aplica a todos os usuários e recursos de Tecnologia da Informação da Administração Pública do Poder Executivo Estadual.

4. Diretrizes

4.1 Os recursos de Tecnologia da Informação devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos, tais como programas antivírus, programas de análise de conteúdo de Correio Eletrônico.

4.2 Havendo correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.

4.3 As atualizações e as correções para os sistemas de detecção e bloqueio de programas maliciosos devem ser homologadas antes de aplicadas ao ambiente de produção.

4.4 É obrigatório o uso de sistemas de detecção e bloqueio de códigos maliciosos em todos os recursos de Tecnologia da Informação.

4.5 Arquivos ou mídias que são utilizados nos equipamentos computacionais devem ser verificados automaticamente, quanto à contaminação por código malicioso, antes de sua utilização.

4.6 Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso.

4.7 Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados pelo *software* antivírus, isolados ou removidos do sistema. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o ambiente de produção.

4.8 Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela área de Tecnologia da Informação do órgão ou entidade.

4.9 Somente mídias magnéticas e produtos de origem confiável devem ser utilizados nos equipamentos computacionais.

5. Competências

5.1 Área de Tecnologia da Informação do Órgão ou Entidade:

5.1.1 auxiliar no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos;

5.1.2 garantir a instalação dos sistemas de detecção e bloqueio de programas maliciosos nos equipamentos computacionais, mantendo-os atualizados, conforme disponibilização do fabricante;

5.1.3 monitorar os logs dos sistemas de detecção e bloqueio de códigos maliciosos, com objetivo de atuar de forma proativa na identificação de ameaças.

5.2 Usuário:

5.2.1 utilizar somente programas homologados;

6. Documentos Relacionados

- ABNT NBR ISO/IEC 27002:2013– Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- Norma 06 - Gerenciamento de Incidentes de Segurança da Informação.

7. Data de Revisão

- 23/11/2015

Norma 17 - Uso de Dispositivos Móveis

1. Objetivo

Proteger os recursos computacionais disponibilizados pela administração pública do poder executivo estadual contra a ação de códigos maliciosos, códigos móveis e programas impróprios, através da definição de regras, critérios de acesso e soluções visando prevenir incidentes de segurança para a organização.

2. Definições

Antivírus: programa (*software*) especificamente desenvolvido para detectar, anular e eliminar vírus e outros tipos de códigos maliciosos.

BYOD: (*Bring Your Own Device* – tradução: "traga seu próprio dispositivo") termo utilizado para definição da prática do uso de dispositivos móveis, de propriedade do colaborador, nas instalações físicas da Organização para realização de atividades laborais.

Código Malicioso (*malware*): termo genérico que se refere a todo tipo de programa especificamente desenvolvido para executar ações danosas em um computador ou outros dispositivos eletrônicos, a exemplo de: vírus, cavalos de tróia, *spyware*, *backdoors*, *keyloggers*, *worms*, *bots* e *rootkits*.

Código Móvel: código executado localmente, proveniente de um sistema remoto de baixa confiabilidade, que executa automaticamente funções específicas com pequena ou nenhuma interação por parte do usuário.

Conformidade: aderência a um padrão previamente estabelecido e aceito como ideal.

Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre.

Dispositivos Móveis: equipamento ou acessório portátil, capaz de se conectar a internet e/ou armazenar dados, tais como: celular, *smartphone*, *tablet*, notebook, netbook, pendrive, CD/DVD e outros semelhantes.

Domínio: Referência que define um nome para o serviço de autenticação dos usuários em uma rede. O nome dado ao domínio, normalmente é usado para fazer referência a rede corporativa da organização.

Informação Sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Rede Corporativa: nomenclatura utilizada para definir os serviços e recursos tecnológicos de uma rede vinculados ao negócio da organização, disponibilizados para os usuários que possuem credencial de acesso no domínio da instituição.

Rede Visitante: nomenclatura utilizada para definir uma rede ou segmento de rede, disponibilizada aos usuários visitantes, com serviços limitados e acesso restrito aos serviços e recursos tecnológicos da rede corporativa.

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública do Poder Executivo Estadual em local ou jornada de trabalho para este último.

Usuário de dispositivo móvel: todo colaborador seja ele servidor, estagiário ou prestador de serviço que acessa, através de dispositivos móveis, informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela Administração Pública Estadual.

Usuário Visitante: Qualquer usuário sem vinculo com o órgão ou entidade da administração pública estadual que necessite acessar, de forma temporária, recursos computacionais da organização.

Vulnerabilidade: fragilidade de um *software*, sistema operacional ou outro componente da infraestrutura de Tecnologia da Informação que pode ser explorada por uma ou mais ameaças internas ou externas à organização.

3. Abrangência

Todos os usuários com dispositivos móveis (de propriedade da organização ou próprio) que desejem acessar os recursos computacionais da organização.

4. Diretrizes

4.1 A fim de viabilizar o cumprimento desta Norma, nos casos em que for permitido o acesso utilizando dispositivo móvel, a organização reserva-se o direito de, através das áreas competentes:

4.1.1 Instalar *software* ou agente para monitorar a utilização e o acesso dos dispositivos móveis aos recursos computacionais da organização;

4.1.2 Auditar, quando necessário, os dispositivos móveis disponibilizados pela organização;

4.1.3 Todos os dispositivos móveis utilizados como estação de trabalho (notebook, netbook, tablet, etc), devem se autenticar no domínio da organização, para ter acesso aos recursos da rede corporativa.

4.2 O usuário de dispositivos móveis corporativos, tem responsabilidade sobre todo e qualquer conteúdo armazenado, e também pela integridade dos mesmos.

4.3 Acesso à Internet

4.3.1 É vedado o uso de modem em equipamento conectado à rede da organização para acesso direto a redes externas, inclusive Internet, nas dependências da organização, salvo para a realização de testes específicos pelas áreas técnicas competentes. O acesso às redes externas deve ocorrer através da arquitetura segura existente e homologada pela organização;

4.3.2 É vedado o uso do serviço de ancoragem / roteamento dos dispositivos móveis com equipamentos conectados à rede corporativa;

4.3.3 Ressalvados os interesses da Administração Pública Estadual é vedado fazer *download* ou *upload* de arquivos através dos recursos da organização cuja utilização ou conteúdo não estejam relacionados às atividades profissionais do usuário de dispositivo móvel, especialmente aqueles que possam representar risco à segurança do ambiente operacional da organização, tais como, mas não limitados a:

a) arquivos de áudio e vídeo;

b) arquivos anexados a mensagens cujos remetentes não são identificáveis ou confiáveis;

c) arquivos multimídia;

d) arquivos executáveis.

4.3.4 Todos os usuários que utilizam recursos da organização para acesso à Internet, devem se autenticar na rede visitante.

4.4 Uso Adequado de Dispositivos Móveis Corporativos

4.4.1 Quando conectados à rede corporativa da organização os dispositivos móveis devem ser configurados e utilizados de forma a reduzir a probabilidade de atuação de códigos maliciosos. Desta forma, as seguintes diretrizes devem ser observadas:

a) Os dispositivos móveis devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos e prevenção e detecção de acesso não autorizado;

b) Com base no conceito de BYOD, a organização deve disponibilizar uma solução de gerenciamento de todos os dispositivos móveis que acessem os recursos computacionais da organização;

c) Qualquer dispositivo móvel que for conectado à uma estação de trabalho deverá ser submetido à verificação do *software* de antivírus, visando detectar à existência de códigos maliciosos e códigos móveis;

d) Não são permitidos a manipulação e armazenamento de músicas, filmes, fotos e software objeto de direitos autorais sem a devida autorização, ou qualquer outro tipo de operação ilegal semelhante, para os dispositivos móveis pertencentes à organização;

e) Não é permitido o armazenamento de informações consideradas sigilosas, em dispositivos móveis sem a devida proteção de segurança, a exemplo do uso de senhas de acesso ao dispositivo, recursos de criptografia ou outra solução adequada para proteção;

f) Documentos criados fora da rede corporativa deverão ser copiados para o ambiente corporativo;

g) Dispositivos móveis cedidos pela organização devem usar, exclusivamente: software homologado e adequadamente licenciado, ou software gratuito autorizado pela organização.

4.4.2 O simples fato da organização permitir acesso ou uso do equipamento ou recursos de informação, por si só, não configura sobreaviso ou sobre jornada do usuário de dispositivo móvel, sendo um ato de liberalidade, proatividade e iniciativa do mesmo;

4.5 Uso de dispositivo móveis de propriedade particular

4.5.1 Nos casos em que o usuário de dispositivo móvel utilize seu equipamento no ambiente de trabalho com fins laborais deverão ser obedecidas as condições e diretrizes de segurança da informação descritas a seguir:

a) O proprietário do equipamento assumirá a responsabilidade por:

- Conteúdo dos arquivos armazenados;
- Licenciamento regular dos softwares instalados, sob pena de responder isoladamente pelo seu uso ilegal;
- Não utilizar software licenciado para uso não comercial, para manipular dados ou informações da organização, sob pena de responder isoladamente pelo seu uso ilegal;
- Sempre utilizar e atualizar os documentos no ambiente da rede corporativa;

b) O equipamento estará sujeito a monitoramento e auditoria por parte da organização;

c) O equipamento estará à disposição da organização como beneficiária de uso temporário e parcial, sem que isso gere qualquer ônus ou responsabilidade para a referida organização;

d) A organização não será responsabilizada pela perda, deterioração, furto, extravio ou quebra do equipamento, e se isso vier a ocorrer o proprietário deverá avisar à organização imediatamente;

e) A organização não será responsável por realizar manutenções, troca de peças, consertos do equipamento e suas funcionalidades. Estas atividades são de completa responsabilidade do proprietário, salvo interesses da administração pública estadual;

f) A organização não será responsável por realizar instalações, manutenções ou atualizações de *softwares* e suas funcionalidades. Estas atividades são de completa responsabilidade do proprietário, salvo interesses da administração pública estadual nas situações de *softwares* corporativos.

4.6 Usuários visitantes com dispositivos móveis

4.6.1 Devem ser estabelecidos procedimentos de controle e concessão de acesso a visitantes que durante a permanência em instalações de órgãos e entidades da administração pública estadual, necessitem conectar seus dispositivos móveis à rede da organização;

4.6.2 Para ter acesso à rede sem fio o usuário visitante deve ser identificado de forma única.

4.7 Termo de Uso e Responsabilidade

4.7.1 Os usuários devem ser orientados a respeito dos procedimentos de segurança acerca dos dispositivos móveis corporativos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade do órgão ou entidade a que pertencem. Não será admitida a alegação de seu desconhecimento nos casos de uso indevido.

5. *Competências*

5.1 **Área de Tecnologia da Informação do Órgão ou Entidade:**

5.1.1 Propor, disseminar e atualizar as diretrizes sobre o uso de dispositivos móveis nas instalações da organização;

5.1.2 Acompanhar e recomendar a adoção de medidas e procedimentos de segurança, visando assegurar o uso adequado de dispositivos móveis na organização;

5.1.3 prover os recursos necessários ao cumprimento desta Norma;

5.2 **Gestor da Área do Usuário:**

5.2.1 comunicar à área de tecnologia da informação do órgão ou entidade todas as movimentações de pessoal que impliquem em concessão, mudança ou revogação de acessos;

5.2.2 comunicar à área de Tecnologia da informação do órgão ou entidade sempre que tomar ciência de direitos de acesso desnecessários à execução das atividades por parte de seus subordinados ou de terceiros;

5.3 **Usuários:**

5.3.1 Utilizar adequadamente os dispositivos móveis conectados na rede da organização, tomando os cuidados necessários para tal, conforme diretrizes estabelecidas nesta Norma.

5.3.2 Comunicar, imediatamente, à área de atendimento ao usuário sobre qualquer ocorrência de perda ou avaria do dispositivo móvel.

5.3.3 Cumprir com os requisitos de segurança estabelecidos nesta Norma.

5.3.4 Manter, de forma adequada, todos os dispositivos móveis sob sua responsabilidade, sendo responsável por todo e qualquer conteúdo armazenado.

6. *Documentos relacionados*

- ABNT NBR ISO/IEC 27002:2013– Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação.
- Norma 03 - Uso da Internet.
- Norma 05 - Acesso e Utilização do Correio Eletrônico.

CONCLUSÃO

Há uma percepção visível do aumento no número de ataques e explorações de vulnerabilidades de segurança, realizado por grupos que têm como alvo corporações de todos os tipos e, em especial, Organizações Governamentais de diversos países, incluindo o Brasil. A adoção deste conjunto de Normas servirá como guia aos gestores dos diversos órgãos e entidades da Administração Pública do Poder Executivo Estadual para o fortalecimento da Segurança da Informação no âmbito do Governo da Bahia, e é essencial no combate a ações que possam causar grandes prejuízos financeiros e políticos ao Estado.

Este documento pretende apoiar o processo de normatização e organização da Gestão da Segurança da Informação no Estado da Bahia com o objetivo de elevar o nível de segurança dos ativos dos órgãos e entidades que compõem a Administração Pública do Poder Executivo Estadual, e deverá receber novas versões com diretrizes revistas e atualizadas, em um processo contínuo de melhoria da sistemática de segurança do Estado.