Tribunal de Contas do Estado do Amazonas

Manual de Rotinas de Segurança da Informação

MRSI-TCE/AM

1ª Edição

2019

A

Yara Amazônia Lins Rodrigues dos Santos
Presidente do TCE/AM

Pela percepção de estruturar o Tribunal de Contas do Estado do Amazonas para caminhar da forma mais acertada no ambiente VICA (volátil, incerto, complexo e ambíguo) de nosso tempo.

Autoria e Organização

Carlos Alberto Souza de Almeida
Procurador de Contas

ÍNDICE TEMÁTICO

Portaria de Implantação.....7
Prefácio.....9
1. SegurançaOrgânica.....11
1.1 Conceito.....11
1.2 Concepção.....11
1.3 Composição.....11
1.4 Segurança dos Recursos Humanos.....11
1.5 Conceito.....11
1.6 Considerações Gerais.....11
1.7 Medidas de Segurança dos Recursos Humanos.....12
1.8 Segurança do Material.....12
1.9 Conceito.....12
1.10 Medidas de Segurança do Material.....12
1.11 Segurança das Áreas e Instalações.....12
1.12 Conceito.....13
1.13 Considerações Gerais.....13
1.14 Medidas das Áreas e Instalações.....13
1.15 Demarcação de Áreas.....13
1.16 Implementação de Barreiras.....13
1.17 Principais Aspectos Considerados na
Definição de Barreiras.....13
1.18 Estabelecimento de Linhas de Proteção.....14
1.19 Adoção de Controle de Acesso.....14
1.20 Emprego de Normas e Procedimentos
Adicionais de Segurança.....15
1.21 Emprego de Equipamentos de Segurança.....15
1.22 Estabelecimento de Proteção Elétrica.....15
1.23 Proteção do Cabeamento.....16
2.0 Segurança da Informação.....17
2.1 Conceito.....17
2.3 Considerações Gerais.....17
2.4 Princípios da Segurança da Informação.....17
2.5 Regras Gerais da Segurança da Informação.....18
2.6 Classificação e Controle.....18
2.7 Composição da Segurança da Informação.....19
2.8 Segurança da Informação no Pessoal.....19
2.9 Medidas de Segurança no Processo Seletivo.....20

2.10 Medidas de Segurança no Desempenho
da Função.....20
2.11 Medidas de Segurança no Desligamento.....21
2.12 Segurança da Informação na Documentação.....21
2.13 Segurança na Produção.....21
2.14 Segurança na Expedição e na Recepção.....22
2.15 Segurança no Manuseio.....22
2.16 Segurança no Arquivamento.....23
2.17 Segurança na Eliminação.....24
2.18 Segurança da Informação no Material.....24
2.19 Segurança de Material em trânsito.....25
2.20 Segurança de Equipamentos fora das
instalações.....25
2.21 Reutilização e Alienação segura de
Equipamentos.....25
2.22 Remoção de Propriedade.....26
2.23 Segurança da Informação nos meios de
Tecnologia da Informação e Comunicações (MTIC).....26
2.24 As Medidas de Prevenção.....26
2.25 Medidas de Segurança Física da Informação
nos meios de Tecnologia da Informação e
Comunicações (MTIC).....27
2.26 Segurança de Software e de Sistemas.....28
2.27 Medidas de Segurança de Acesso à
Informação nos meios de TIC.....28
2.28 Cuidados no uso da senha.....31
2.29 Medidas de Segurança de Conteúdo da
Informação nos MTIC.....32
2.30 Criptografia.....32
2.31 Autenticação de Mensagens.....33
2.32 Assinatura Digital.....33
2.33 Serviços de Irretratabilidade (não repúdio).....33
2.34 Outras técnicas.....34
2.35 Medidas de Segurança de Transmissão
da Informação nos MTIC.....34
2.36 Medidas a serem executadas:.....34
2.37 Esteganografia.....34
2.38 Segurança dos Sistemas de Automação
de documentos.....35
2.39 Segurança de Redes de Computadores.....36

2.40 Segurança no Correio Eletrônico.....36
2.41 Trabalho remoto.....37
2.42 Procedimentos de Backup.....38
2.43 Auditorias e Tratamento de Incidentes.....38
2.44 Medidas de Segurança da Informação em
Mídias Sociais e em Aplicativos de TI.....39
2.45 Medidas de Segurança da Informação
nos Aparelhos de Telefonia Celular.....39
2.46 Segurança da Informação nas Áreas
e Instalações.....39
Termo de Compromisso de Manutenção
de Sigilo (TCMS).....41
Apêndice 1 – Sugestões sobre Segurança
Orgânica.....43
Apêndice 2 – Procedimentos de Mesas e
Telas Limpas.....45
Termos e Definições.....47

PORTARIA Nº 1/2019 – GP/CGSI TCE/AM de 04 de novembro de 2019

Aprova o Manual de Rotinas de Segurança da Informação MRSI-TCE/AM -2019, 1ª Edição, e dá outras providências.

A Presidente do Tribunal de Contas do Estado do Amazonas, no uso das atribuições legais e regimentais que lhe confere, resolve:

Art. 1º. Aprovar o Manual de Rotinas de Segurança da Informação MRSI-TCE/AM -2019, 1ª Edição.

Art. 2º. Revogar qualquer disposição em contrário.

Art. 3º. Determinar que esta Portaria entre em vigor na data de sua publicação.

Yara Amazônia Lins Rodrigues dos Santos
Conselheira-Presidente do Tribunal de Contas
do Estado do Amazonas

PREFÁCIO

O Tribunal de Contas do Estado do Amazonas atento às ameaças e aos conflitos de um tempo onde o conhecimento é a maior riqueza dos povos, busca a implantação de uma doutrina de planejamento e emprego das regras de resguardo e cautela do seu acervo informações, materializadas nos autos de processos, nas denúncias e representações que recebe, nas estratégias investigativas de seus agentes, nos planos de trabalhos e achados de auditorias, nos votos de seus julgadores.

O combate aos ilícitos vem sofrendo mudanças no tempo, assim como as ameaças e contraventores. The Phantom, Flash Gordon, irmãos Earp e Doc Holliday combatiam inimigos identificados, como monstros, Clantons e McLaurys. Suas armas eram espadas, pistolas e – num exercício de futurismo – laser.

O salto tecnológico trouxe novos atores e armas. No ano de 2019, divulgou-se que 5% (cinco por cento) da produção de petróleo do planeta, na Arábia Saudita, foi travada pela ação de drones kamikases, comandados por homens que os dirigiam – alhures – por meio de computadores.

Mudaram os valores, os perfis inimigos, mudaram as armas de combate, e mais, paradoxalmente, a constante é a mudança.

Este manual, iniciativa do CGSI (Comitê Gestor de Segurança da Informação) do TCE-AM, descreve rotinas e modificações conceituais impostas pela necessidade de atualização, em sintonia com as mais novas regras de cautela e resguardo das informações adotadas pelas grandes organizações.

Dessa forma, este manual visa a fornecer uma ferramenta de trabalho atualizada e útil para uso do TCE/AM, em toda sua estrutura orgânica, particularmente para a área de Tecnologia da Informação.

1. SEGURANÇA ORGÂNICA

1.1 CONCEITO

A Segurança Orgânica preconiza a adoção de um conjunto de medidas destinado a prevenir e obstruir possíveis ameaças de qualquer natureza dirigidas contra pessoas, dados, informações, materiais, áreas e instalações.

1.2 CONCEPÇÃO

A Segurança Orgânica implica a adoção de postura preventiva por todos os servidores, sendo necessária a criação, o desenvolvimento e a manutenção de uma mentalidade de proteção em toda a estrutura hierárquica, visando à obtenção de um grau de proteção ideal.

No estabelecimento da Segurança Orgânica, os seguintes aspectos são levados em consideração:

I - os meios disponíveis;
II - as deficiências;
III - as ameaças; e
IV - o grau de segurança ideal a ser obtido.

1.3 COMPOSIÇÃO

Para atingir o grau de segurança desejado, a Segurança Orgânica é composta pelos seguintes grupos de medidas:

I - Segurança dos Recursos Humanos;
II - Segurança do Material;
III - Segurança das Áreas e Instalações; e
IV - Segurança da Informação.

As medidas de Segurança Orgânica devem ser conhecidas, adotadas e praticadas por todos os agentes públicos.

1.4 SEGURANÇA DOS RECURSOS HUMANOS

1. 5 CONCEITO

Consiste no grupo de medidas destinadas a preservar a integridade física e moral dos recursos humanos do TCE/AM.

1.6 CONSIDERAÇÕES GERAIS

Os recursos humanos, bens mais importantes do órgão de Controle Externo, precisam ser protegidos e preservados.

A permanência por elevado tempo no desempenho de atividades sensíveis representa um risco a ser considerado. Para minimizá-lo, será efetuada, sempre que se mostre possível e necessário, a troca dos servidores que desempenham essas funções.

1.7 MEDIDAS DE SEGURANÇA DOS RECURSOS HUMANOS

A fim de assegurar um grau de segurança ideal no que concerne à proteção do pessoal, são adotadas medidas para fazer face às ameaças a esse ativo, considerando-se:

a) a possibilidade de envolvimento de integrantes do público interno como vítimas de ilícitos ou irregularidades;

b) a espionagem, que pode utilizar-se de servidores, tanto como agentes infiltrados quanto pela exploração de suas eventuais deficiências;

c) a ação hostil, que atente contra a integridade física de integrantes do público interno;

d) os acidentes, de qualquer natureza, que podem causar danos ao pessoal, incluindo-se os fenômenos naturais.

1.8 SEGURANÇA DO MATERIAL

1.9 CONCEITO

Consiste no grupo de medidas voltadas à proteção do material, de forma direta ou indireta.

As ações de sabotagem constituem, também, uma ameaça, podendo provocar a perda do material ou sua indisponibilidade.

1.10 MEDIDAS DE SEGURANÇA DO MATERIAL

As medidas de Segurança do Material abrangem a guarda do material em condições técnicas adequadas e em instalações apropriadas, segundo os manuais técnicos e as possibilidades das ameaças.

Danos ao material podem decorrer de atos não intencionais, ou não, bem como de fenômenos naturais.

Os equipamentos e outros materiais relevantes são instalados e protegidos, visando a reduzir os riscos decorrentes de ameaças de qualquer natureza.

1.11 SEGURANÇA DAS ÁREAS E INSTALAÇÕES

1.12 CONCEITO

Consiste no grupo de medidas voltadas para os locais em que ocorram atividades humanas ou nos quais são elaboradas, tratadas, manuseadas ou guardadas informações e materiais, com a finalidade de salvaguardá-los.

1.13 CONSIDERAÇÕES GERAIS

A implementação da Segurança das Áreas e Instalações exige o cumprimento de medidas de segurança relativas às áreas, edificações e instalações, em particular os locais que contenham informação classificada ou sob restrição de acesso, e os materiais de acesso restrito.

Os fenômenos naturais, os acontecimentos fortuitos e os atos praticados (por ação ou omissão), ainda que sem objetivo deliberado de causar danos, também são considerados no que tange à Segurança das Áreas e Instalações.

1.14 MEDIDAS DE SEGURANÇA DAS ÁREAS E INSTALAÇÕES

1.15 Demarcação das Áreas

Tem por objetivo identificar as áreas de acesso restrito, por meio de sinalizações de fácil entendimento, apresentando-se como um primeiro elemento dissuasor à quebra de segurança.

1.16 Implementação de Barreiras

Barreiras são obstáculos, de qualquer natureza, para impedir o ingresso de pessoas não autorizadas nas áreas de acesso restrito e permitir um efetivo controle da circulação das pessoas que possuam autorização para tal.

As barreiras podem ser físicas (cercas, muros, guardas ou animais) ou conceituais (áreas com acesso restrito, faixas delimitadoras pintadas etc.).

1.17 Principais aspectos considerados na definição das barreiras:

a) a proteção deve ser compatível com os riscos identificados;

b) a proteção física pode ser alcançada, por intermédio da criação, se possível, de barreiras sucessivas em torno da área do órgão ou de parte de suas instalações, de modo que cada linha de barreira estabeleça um perímetro de segurança;

c) a localização e a capacidade de cada barreira dependem do Exame de Situação;

d) qualquer barreira só será efetiva se complementada por outras medidas; e

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

1.18 Estabelecimento de Linhas de Proteção

As linhas de proteção compartimentam ambientes, salas e corredores. Além disso, definem acessos de maior ou menor restrição, para os integrantes dotados de credencial de segurança.

Sob o aspecto físico, admite-se a necessidade de proteção de áreas e instalações e, ainda, que estas possam estar inclusas em um perímetro de segurança, como um determinado setor de vigilância.

1.19 Adoção de Controle de Acesso

É um processo que seleciona o acesso de pessoas a qualquer área ou objeto específico.

Tem por objetivo prevenir o comprometimento das informações e instalações físicas do órgão. Para isso, os recursos e as instalações são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras apropriadas e controle de acesso.

As áreas de segurança devem ser protegidas por controles de entrada apropriados, de modo a assegurar que apenas pessoas autorizadas tenham acesso.

O controle de acesso baseia-se na identificação e na avaliação dos graus de autorização de entrada e saída, sendo feito, normalmente, por meio de uma ou mais das seguintes medidas:

a) uso de meios adequados pela pessoa que pretenda acessar a área ou instalação, tais como chave, crachá, cartão magnético ou símbolo;

b) uso de senha ou código;

c) identificação de partes físicas do corpo humano (íris, digitais, entre outras); e

d) combinação desses meios.

Os sistemas de controle de acesso variam, desde fechaduras até dispositivos que realizam análises biométricas, passando por uma infinidade de sistemas baseados em cartões, teclados digitais e scanners.

1.20 Emprego de Normas e Procedimentos Adicionais de Segurança

Normas e procedimentos adicionais são usados para melhorar as condições de segurança das áreas de acesso restrito. Isso inclui controles para o pessoal do órgão, para terceiros que trabalham em áreas de acesso restrito, assim como para atividades terceirizadas, que possam ocorrer nessa área.

Os seguintes itens são considerados:

a) conhecimento, pelos integrantes do órgão, da existência de área de segurança ou que permita atividades dentro dela apenas quando necessário;

b) evitar o trabalho sem supervisão nas áreas de segurança;

c) fechamento físico e fiscalização periódica das áreas de segurança desocupadas;

d) restrição de acesso do pessoal de serviço às áreas de segurança, sendo autorizado somente quando as atividades o exigirem. Esse acesso também deve ser monitorado; e

e) proibição do uso de equipamentos fotográficos, de vídeo, de áudio ou de outro equipamento de gravação, particularmente telefone celular, em qualquer área ou atividade do órgão considerada sensível.

As autorizações eventuais para emprego desses aparelhos são submetidas à criteriosa análise, considerando a necessidade e a segurança.

1.21 Emprego de Equipamentos de Segurança

Equipamentos de segurança, tais como os equipamentos de combate a incêndio, são instalados com o objetivo de se prevenir perda, dano ou comprometimento dos ativos e a interrupção de atividades.

1.22 Estabelecimento de Proteção Elétrica

Todos os equipamentos elétricos devem ser protegidos contra falhas de energia e outras anomalias na alimentação elétrica.

Algumas medidas para evitar cortes ou falhas no fornecimento elétrico incluem alimentação múltipla, nobreak ou gerador. Essas ações objetivam a continuidade na operação dos sistemas elétricos e eletrônicos.

A iluminação de emergência deve estar disponível em casos de falha na fonte elétrica primária.

É necessário que a proteção contra raios seja usada em todos os pré-

dios; e que filtros de proteção contra raios sejam instalados em todas as linhas de comunicação externas.

1.23 Proteção do Cabeamento

Todo o cabeamento elétrico e de telecomunicação que transmite dados, ou suporta os serviços de informação, deve ser protegido contra interceptação ou danos.

As seguintes ações devem ser consideradas:

a) proteger o cabeamento da rede contra interceptações ou danos;

b) separar os cabos elétricos e os cabos de comunicação, para prevenir interferências;

c) instalar conduítes blindados e salas ou gabinetes trancados nos pontos de inspeção e terminais;

d) usar rotas e meios de transmissão alternativos;

e) instalar cabeamento de fibra óptica;

f) realizar varreduras periódicas, para identificar dispositivos não autorizados conectados aos cabos; e

g) tornar subterrâneas as linhas elétricas e de telecomunicações das instalações de processamento da informação ou submetê-las à proteção alternativa adequada.

2. SEGURANÇA DA INFORMAÇÃO

2.1 CONCEITO

A Segurança da Informação consiste no grupo de medidas destinado a garantir a disponibilidade, integridade, confidencialidade (sigilo), autenticidade, irretratabilidade (não repúdio) e atualidade da informação, em todo o seu ciclo de vida.

2.3 CONSIDERAÇÕES GERAIS

A Informação é um recurso vital para o adequado funcionamento de toda e qualquer órgão da Administração, sendo tratada como ativo a ser protegido.

A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, mostrada em filmes ou difundida verbalmente. Seja qual for a sua forma, ou o meio pelo qual é compartilhada ou armazenada, é necessário que a informação seja protegida.

Dessa forma, a Segurança da Informação atua objetivamente sobre os suportes da informação, que são as pessoas, os documentos, os materiais, os meios de tecnologia da informação e comunicações, as áreas e as instalações.

A Segurança da Informação é obtida a partir da implementação de uma série de controles estabelecidos para garantir que os objetivos de segurança específicos sejam atendidos.

A Segurança da Informação deve estar em conformidade com os requisitos legais e as normas internas do TCE/Am. Ressalte-se a importância dos direitos de propriedade intelectual, proteção de dados, privacidade da informação pessoal e prevenção do uso indevido de facilidades de processamento da Informação.

2.4 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é caracterizada pela preservação dos seguintes princípios:

a) Confidencialidade (sigilo) – garantia de que o conteúdo da informação só é acessível e interpretável por quem possuir autorização;

b) Integridade – garantia de que o conteúdo original da informação não seja modificado; é a certeza de que a exatidão e a inteireza estejam salvaguardadas;

c) Disponibilidade – garantia de que o conteúdo da informação esteja disponível para quem possuir autorização ou credencial de segurança, sempre que houver necessidade;

d) Autenticidade – certificação de que o conteúdo da informação possua integridade, assim como a fonte geradora tenha sua origem comprovada;

e) Inviolabilidade – garantia de que os meios de proteção da informação não sejam violados; e

f) Irretratabilidade (não repúdio) – garantia de que, num processo de envio e recebimento de informações, qualquer participante, originador ou destinatário de informação, não possa, em um momento posterior, negar a respectiva atuação.

2.5 REGRAS GERAIS DA SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação está diretamente associada à conscientização do público interno, à capacitação dos recursos humanos e à qualidade das soluções adotadas para a proteção das informações.

As ameaças e as deficiências, relativas à segurança dos dados e informações, são consideradas no contexto da crescente informatização de atividades e processos.

Para a otimização da Segurança da Informação, pode ser necessária a participação de outros agentes, como a contratação de consultoria externa especializada ou a realização de assessoria técnica interna.

A adoção de qualquer solução tecnológica, nacional ou estrangeira, para atendimento a requisitos relativos à Segurança da Informação, no âmbito do TCE/AM, é precedida de estudos sobre a sua pertinência, confiabilidade, permanência, manutenção e suporte.

A compartimentação de funções contribui para a redução dos riscos para a segurança da informação.

São avaliados os riscos decorrentes do acesso de terceiros a dados e informações sensíveis, inclusive aos seus suportes.

É necessário que os requisitos de segurança resultantes do acesso de terceiros (incluídos os prestadores de serviço que trabalhem no órgão) constem nos contratos firmados, particularmente, no que tange à assinatura do Termo de Compromisso de Manutenção do Sigilo (TCMS).

2.6 CLASSIFICAÇÃO E CONTROLE

Classificação é o ato de se atribuir grau de sigilo à informação que requeira medidas especiais de salvaguarda e, por consequência, aos seus suportes.

A informação é classificada para indicar sua importância, prioridade e tratamento.

Um conjunto de medidas é definido para rotular e tratar a informação, de acordo com o processo de classificação adotado pelo TCE/AM. Esses procedimentos precisam abranger tanto a informação no formato físico quanto no digital.

Para cada classificação, é necessário que procedimentos de tratamento sejam definidos para abranger os seguintes tipos de atividade de processamento da informação:

a) produção;
b) cópia e manuseio;
c) armazenamento;
d) transmissão; e
e) eliminação.

2.7 COMPOSIÇÃO DA SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação compreende os seguintes subgrupos de medidas:

a) Segurança da Informação no Pessoal;

b) Segurança da Informação na Documentação;

c) Segurança da Informação no Material;

d) Segurança da Informação nos Meios de Tecnologia da Informação e Comunicações; e

e) Segurança da Informação nas Áreas e Instalações.

2.8 Segurança da Informação no Pessoal

Consiste no subgrupo de medidas destinadas a assegurar comportamentos, no público interno, adequados à proteção de dados e informações de natureza institucional.

A Segurança da Informação no Pessoal é baseada nas seguintes premissas:

a) a necessidade de conhecer está ligada à função desempenhada;

b) o acesso à informação sensível é permitido apenas às pessoas que tenham necessidade de conhecer;

c) o acesso às informações classificadas, ou sob restrição de acesso, é permitido apenas às pessoas credenciadas ou que tenham assinado o TCMS; e

d) o conhecimento de assunto sensível depende da função; e não do grau hierárquico.

São implementadas ações com o objetivo de desenvolver a mentalidade de cautela e resguardo no público interno, com foco na Segurança da Informação.

Para efeito de sua aplicação, as medidas de Segurança da Informação no Pessoal estão agrupadas em Segurança no Processo Seletivo, no Desempenho da Função e no Desligamento.

2.9 Medidas de Segurança no Processo Seletivo – visam a dificultar a infiltração e a admissão de indivíduos com potencial para comprometer a segurança de dados e informações. Medidas a serem executadas:

a) avaliação da sensibilidade da função – essa medida é tomada tendo em vista que as diversas funções exercidas nos setores do órgão, possuem um grau de sensibilidade decorrente do valor dos ativos a elas atinentes. Em decorrência dessa avaliação, são determinadas as características pessoais julgadas necessárias para o desempenho dessas funções, sob o ponto de vista da cautela e do resguardo; e

b) investigação de segurança – essa medida visa a assegurar que os recursos humanos selecionados possuam os atributos necessários para o desempenho das funções consideradas sensíveis.

2.10 Medidas de Segurança no Desempenho da Função – visam a validar o credenciamento, proceder à educação de segurança e confirmar as características pessoais exigidas.

Problemas pessoais e financeiros, mudanças de comportamento ou estilo de vida, ausências frequentes e sinais de estresse ou depressão podem levar a fraudes, roubos, erros ou outros riscos.

Medidas a serem executadas:

a) credenciamento de segurança – confirmadas as exigências de segurança inerentes à função, é expedida a credencial de segurança apropriada, por meio de ato administrativo exarado por autoridade competente, estabelecendo o grau de sigilo a que o credenciado poderá ter acesso. Essa credencial de segurança pode ser alterada em função de novas necessidades relativas à mesma função ou outra para a qual o servidor for designado;

b) educação de segurança – é necessário que os integrantes do órgão sejam treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação;

c) assinatura do TCMS – o acesso a documento ou material sob restrição de

acesso exige a assinatura de TCMS, conforme a necessidade de conhecer; e

d) resposta aos incidentes de segurança e ao mau funcionamento – os incidentes que afetam a segurança são notificados, por meios de canais apropriados, o mais rapidamente possível.

Todos os integrantes do órgão são orientados a notificarem eventuais incidentes que possam gerar impactos na segurança. Esses incidentes devem ser registrados e informados a autoridade superior, visando ao aprimoramento da segurança.

2.11 Medidas de Segurança no Desligamento

a) A segurança no desligamento visa a salvaguardar informações sigilosas, após o desligamento.

b) Os TCMS ficam arquivados, normalmente, após o desligamento, por tempo indeterminado, estendendo as responsabilidades pela Segurança da Informação.

2.12 Segurança da Informação na Documentação

A Segurança da Informação na Documentação consiste no subgrupo de medidas aplicadas à documentação, destinadas a evitar o seu comprometimento, visando à salvaguarda de dados, informações ou conhecimentos, de caráter sigiloso ou não, que devam ser protegidos.

Os documentos, historicamente, constituem o suporte mais comum das informações, tornando-se alvos permanentes das ações hostis, em particular da espionagem e da sabotagem.

O comprometimento pode ocorrer, ainda, em decorrência de fenômenos naturais e, até mesmo, por ações executadas sem objetivo deliberado de afetar a informação.

Os documentos possuem um ciclo de vida que pode ser desdobrado nas seguintes etapas: produção; expedição; recepção; manuseio; arquivamento; e eliminação.

2.13 a) Segurança na Produção – as medidas de segurança na produção visam à atribuição de grau de sigilo, ao controle dos recursos utilizados na produção de documentos sigilosos e à marcação desses documentos com sinais de segurança (paginação, autenticação, marca d'água etc.).

Medidas a serem executadas:

1) atribuição preliminar de restrição de acesso – atribuir essa restrição ao do-

cumento ou material em fase de produção, levando em consideração fatores como natureza do assunto, finalidade, usuário e aspectos essenciais nele contidos;

2) controle dos recursos utilizados – recursos utilizados na elaboração de documentos sigilosos, tais como rascunhos, notas, carbonos e desenhos, são objeto de controle de segurança pelos seus responsáveis. Normalmente, esses recursos são destruídos após a sua utilização ou, quando não for o caso, são objeto de cuidados especiais relativos à sua segurança;

3) numeração das páginas – visa a contribuir para a integridade do documento, representando um sinal de segurança contra o extravio e a subtração de páginas;

4) classificação – tem por objetivo proteger a informação que requeira medidas especiais de salvaguarda, atribuindo-lhe grau de sigilo; e

5) restrição de acesso – será mantido sob restrição de acesso, independentemente de classificação, o documento, a área ou a instalação sob a competência do TCE/Am.

2.14 b) Segurança na expedição e na recepção – as medidas de segurança na expedição e na recepção visam a estabelecer controles de segurança na tramitação dos documentos.

Medidas a serem executadas:

1) autenticação de documento – processo utilizado para confirmar ou garantir ao usuário a identidade de uma pessoa ou organização, garantindo a fidelidade da fonte e confirmando a procedência da documentação;

2) acondicionamento do documento – estabelecimento de procedimentos adicionais de segurança do documento a ser expedido, permitindo a identificação de indícios de eventual comprometimento;

3) controle de saída – adoção de registros de saída, atribuindo-se responsabilidades pela expedição e pelo tráfego do documento sigiloso, para possibilitar o eficaz controle da difusão; e

4) controle de entrada – adoção de controles da recepção e tramitação interna dos documentos sigilosos recebidos. Envolve procedimentos relativos à inspeção do acondicionamento e à autorização para abertura de invólucros, assinatura de recibos, distribuição interna, abrangendo todos os tipos de registros que possibilitem a apuração de responsabilidades, quando da constatação de comprometimento.

2.15 c) Segurança no manuseio – as medidas de segurança no manuseio visam a estabelecer procedimentos para reprodução, custódia e classi-

ficação, desclassificação ou reclassificação de documentos sigilosos, permitindo implementar controles de segurança, durante sua utilização.

Medidas a serem executadas:

1) controle de reproduções – a cópia ou o extrato de documento classificado ou sob restrição de acesso receberá um código numérico ou alfanumérico específico (controle de vazamento) para cada destinatário, a fim de identificar a origem de um possível vazamento e facilitar o seu controle. Esse código será colocado no corpo do texto, em todas as páginas do documento, sendo visível e de fácil identificação. No documento original, constará a relação de todos os destinatários com os seus respectivos códigos;

2) controle de custódia – enquanto o documento sigiloso permanecer com o usuário, são estabelecidos procedimentos cautelares visando ao seu efetivo controle;

3) classificação, desclassificação ou reclassificação – conforme estabelecido na legislação vigente; e

4) seleção dos documentos a serem arquivados ou eliminados – para determinação da destinação final dos documentos, será observada a legislação vigente.

2.16 d) Segurança no arquivamento – as medidas de segurança no arquivamento visam a definir os locais e processos adequados de arquivamento e recuperação dos documentos sigilosos e estabelecer rotinas para situações de emergência.

Medidas a serem executadas:

1) escolha do local – selecionar o local adequado, sob o enfoque de segurança, para a instalação dos arquivos que abrigam documentos sigilosos. Entre outras, impõem-se as providências quanto à circulação de pessoas e ao deslocamento da documentação em casos de emergência;

2) escolha do tipo de arquivo ou cofre – o tipo de arquivo ou cofre decorre da avaliação do modelo adequado para abrigar os documentos de diferentes graus de sigilo;

3) controle no arquivamento e na recuperação – é efetivado pelo estabelecimento de rotinas para o arquivamento e a recuperação dos documentos nos arquivos. Exige-se a definição de responsabilidades para o manuseio e controle dos documentos sigilosos arquivados; e

4) estabelecimento de rotinas para evacuação em situações de emergência (medidas de contingência) – são instituídos procedimentos relativos à evacuação

da documentação sensível, em situações de emergência. Essas medidas envolvem o estabelecimento de prioridades e responsabilidades e a determinação, antecipada, de locais alternativos para abrigar os documentos a serem salvos.

2.17 e) Segurança na eliminação – as medidas de segurança na eliminação visam, depois de cumprido o ciclo de vida do documento, de acordo com a legislação em vigor, a definir meios e locais de eliminação, a determinar formas de controle, bem como estabelecer rotinas de eliminação para situações de emergências (medidas de contingência).

Medidas a serem executadas:

1) escolha dos meios (material e pessoal) e dos locais a serem utilizados para a eliminação;

2) controle da eliminação – objetiva estabelecer rotinas criteriosas para a efetiva eliminação dos documentos sigilosos julgados inservíveis.

3) estabelecimento de rotinas para eliminação em situações de emergência – visa a evitar a captura de documentos sensíveis por estranhos, em situação crítica.

2.18 Segurança da Informação no Material

A Segurança da Informação no Material consiste no subgrupo de medidas voltadas para proteger as informações contidas em determinados materiais.

Para a Segurança da Informação no Material, toda matéria, substância ou artefato que contenha, utilize ou veicule informações, que, de posse de ator(es) de qualquer natureza, possam implicar riscos para qualquer ativo do TCE/AM devem ser salvaguardados.

O material, em razão da sensibilidade das informações nele contidas, pode tornar-se alvo permanente das ações hostis, em particular da espionagem e de danos.

O comprometimento pode ocorrer, ainda, em decorrência de fenômenos naturais ou de ações desenvolvidas sem objetivo deliberado de afetar a informação contida no material.

Com relação à Segurança da Informação no Material, controlado ou não, são adotadas, no que for aplicável, prescrições similares às da Segurança da Informação na Documentação.

A Segurança da Informação no Material é executada, prioritariamente, por intermédio do cumprimento de regulamentos, instruções ou normas que regem a produção, a classificação, a distribuição, o recebimento, o registro, o manuseio,

a guarda, o armazenamento e acondicionamento e a eliminação de materiais.

2.19 Segurança de material em trânsito – o material classificado ou sob restrição de acesso pode ficar vulnerável à quebra de segurança, uso impróprio ou alteração, durante o seu transporte físico.

Recomenda-se que os seguintes controles sejam aplicados para salvaguardar materiais que estão sendo transportados entre localidades:

1) utilização de transporte ou de serviço de mensageiro confiável;

2) embalagem adequada para proteger o conteúdo contra qualquer dano físico que possa vir a ocorrer durante o transporte e estar de acordo com especificações dos fabricantes; e

3) adoção de controles especiais, quando necessário, para proteger informações sensíveis. Como exemplo, pode-se incluir:

a) utilização de recipientes lacrados (com controle de número de lacre);

b) entrega em mão (com controle de recebimento);

c) utilização de lacre externo de pacotes (que revele qualquer tentativa de acesso);

d) divisão do conteúdo para mais de uma entrega e expedição por rotas distintas em casos excepcionais; e

e) uso de assinatura digital e de criptografia.

2.20 Segurança de equipamentos fora das instalações

a) O uso de qualquer equipamento que contenha informação sensível, fora das instalações do órgão, será previamente avaliado e autorizado.

b) O grau de segurança será, no mínimo, equivalente àquele existente nas instalações do órgão.

c) Os riscos de segurança, tais como dano, roubo e espionagem, podem variar em virtude da localização, impondo o emprego de controles apropriados.

2.21 Reutilização e alienação segura de equipamentos

a) A Informação pode ser exposta pelo descuido na alienação ou reutilização de equipamentos e materiais.\

b) É necessário que dispositivos de armazenamento e materiais que con-

tenham informação sensível sejam destruídos, fisicamente ou sobrescritos de forma segura, ao invés da utilização de funções-padrão para o apagamento.

c) Dispositivos de armazenamento danificados que contenham informação sensível podem necessitar de uma análise para determinar a sua eliminação.

2.22 Remoção de propriedade

a) Equipamentos, informações ou softwares não devem ser retirados do órgão sem autorização.

b) São realizadas inspeções de forma a detectar a remoção não autorizada de propriedade. Todos devem estar cientes de que essas inspeções serão realizadas.

2.23 Segurança da Informação nos meios de tecnologia da informação e comunicações (MTIC)

A Segurança da Informação nos MTIC consiste no subgrupo de medidas destinadas a salvaguardar as informações, bem como a integridade dos sistemas e MTIC do órgão.

A Informação é um dos ativos mais valiosos de uma organização. Grande parte dela está armazenada e é transmitida por meios eletrônicos, em um ambiente complexo, exigindo normas de segurança compatíveis, tais como senhas, sistemas de autenticação e criptografia.

Toda informação classificada ou sob restrição de acesso, que seja armazenada, processada ou trafegue por ambientes de rede de dados é submetida a processos que assegurem a sua disponibilidade, integridade, confidencialidade e autenticidade.

No planejamento de Segurança da Informação nos MTIC é considerada a capacidade da busca dos atores hostis para obtenção de informações.

A busca de dados, informações ou conhecimento exige, além das capacidades de interceptação e armazenamento, capacidade de análise de grande volume de dados, bem como o desenvolvimento de técnicas de criptoanálise.

2.24 As medidas de prevenção são:

a) conhecer as possíveis formas de ataque;

b) buscar a assinatura das listas de segurança;

c) utilizar programas antivírus atualizados e ferramentas de segurança confiáveis;

d) manter o pessoal treinado e atualizado;

e) selecionar o pessoal criteriosamente; e

f) manter mais de um administrador do sistema.

A segurança contra ações hostis abrange, também, as medidas de proteção funcional (treinamento e motivação), administrativas (auditoria e fiscalização), de mídia (inspeção, eliminação, armazenamento, uso e contingência), contra radiação (por intermédio do uso de blindagem) e controle de ciclos (registro de ocorrências e reavaliação das medidas de segurança).

2.25 Medidas de segurança física da informação nos meios de tecnologia da informação e comunicações (MTIC)

a) As medidas de segurança de controle físico visam a proteger o ambiente e os locais onde se encontram os meios de TIC, contra o acesso de pessoas não autorizadas, bem como protegê-los dos riscos naturais ou intencionais.

b) Ainda, são observados, de forma particular, os seguintes procedimentos:

1) armazenagem externa de dados (backup):

a) visa a evitar a interrupção do processamento de dados nos casos de sinistro ou sabotagem dos dados originais; e

b) o local de armazenagem é afastado do arquivo original, de forma a impossibilitar a sua eliminação simultânea.

2) para a preservação da integridade dos dispositivos durante o transporte, são adotadas as seguintes providências:

a) prevenir choques térmicos, choques físicos e desmagnetização;

b) utilizar meios adequados de transporte; e

c) usar malas adequadas, com divisões internas variadas, que sejam protegidas contra choques e radiações.

3) manutenção de MTIC:

a) é executada pelo pessoal especializado do próprio órgão, preferencialmente;

b) qualquer serviço a ser executado em equipamento informatizado por empresa contratada, que contenha assunto classificado ou sob restrição de acesso,

será acompanhado pelo responsável por sua utilização; e

c) o computador que contenha informação classificada ou sob restrição de acesso e que necessite de manutenção fora do órgão terá o seu disco rígido retirado e guardado em um cofre.

2.26 Segurança de software e de sistemas

a) Entre os principais tipos de softwares estão os de sistema operacional, processador de texto, gerenciador de banco de dados, editoração eletrônica, processador gráfico, planilhas eletrônicas e os corporativos.

b) Ao serem instalados nos equipamentos, os softwares possibilitam a interação do usuário com a máquina, por intermédio do sistema implantado, possuindo, na maioria das vezes, pontos críticos de entrada e, até mesmo, de adequados procedimentos relativos a senhas.

c) As medidas de segurança de software são adotadas ou exploradas nos diferentes softwares, para que eles não tenham seus códigos-fonte alterados, instalados ou operados por elementos não credenciados.

d) São utilizados apenas softwares licenciados, de acordo com a legislação em vigor, inclusive os de domínio público, após parecer favorável e assessoramento técnico de pessoal especializado da OM.

e) A instalação de software somente é realizada por pessoal habilitado da OM.

f) O uso de dispositivos móveis, para o trato de informação sensível, é evitado. Caso esse uso seja imprescindível, são adotadas medidas de segurança adicionais (criptografia, uso de contêineres seguros etc.).

2.27 Medidas de segurança de acesso à informação nos meios de TIC

a) É necessário que os acessos à informação e aos processos do órgão sejam controlados por meio de normas de segurança, levando-se em consideração as regras para autorização e difusão da informação.

b) As regras de controle de acesso e de direitos, para cada usuário ou grupo de usuários, são claramente estabelecidas.

c) O gerenciamento de acessos do usuário aos sistemas de informação proporciona, no mínimo:

1) registro de usuário (procedimento formal de registro e cancelamento de usuário para obtenção de acesso) e definição das suas responsabilidades;

2) gerenciamento de privilégios, pelo controle de níveis de acesso ao sistema ou aplicação;

3) gerenciamento de senha dos usuários;

4) controle de acesso à rede;

5) compartimentação do acesso, permitindo que os usuários acessem apenas os serviços especificamente autorizados;

6) rota de rede obrigatória entre o terminal do usuário e o serviço do computador;

7) autenticação para conexão externa do usuário e de nó;

8) controle de conexões de rede e proteção de portas de diagnóstico remotas; e

9) compartimentação (segmentação) de redes.

d) Os computadores são configurados para encerrar automaticamente as sessões, por meio de “tempo limite de sessão”.

e) O acesso aos computadores é protegido por meio de protetor de tela e senha.

f) Os requisitos das normas de controle de acesso para redes compartilhadas, especialmente aquelas que se estendem além dos limites do órgão, podem requerer a incorporação de controles que limitem a capacidade de conexão dos usuários. Tais controles podem ser implementados por meio de firewall de rede, que filtram o tráfego usando tabelas ou regras predefinidas. Entre as redes que necessitam de restrições, destacam-se as aplicações de correio eletrônico, as de transferência unidirecional e bidirecional de arquivos, as de acesso interativo e as que permitem o acesso de acordo com a hora.

g) O acesso às redes de computadores é protegido com a utilização de usuários e senhas, possibilitando a segregação de acesso às informações.

h) As funcionalidades de segurança dos sistemas são usadas para restringir o acesso aos recursos computacionais e às informações. É necessário que estas funcionalidades permitam:

1) identificação, autenticação e verificação da identidade e, se necessário, do terminal e da localização de cada usuário autorizado;

2) registro dos sucessos e das falhas de acesso ao sistema;

3) fornecimento de meios apropriados para a autenticação - se um sis-

tema de gerenciamento de senhas for usado, é necessário que ele garanta o cadastramento de senhas seguras;

4) restrição do tempo de conexão dos usuários, quando apropriado;

5) procedimentos de entrada e saída no sistema (logon/logoff);

6) desconexão de terminal por inatividade;

7) controle do acesso dos usuários à informação e às funções dos sistemas de aplicação, de acordo com as normas definidas pelo órgão;

8) proteção contra acesso não autorizado para qualquer software que seja capaz de sobrepor-se aos controles das aplicações ou do sistema;

9) o não comprometimento da segurança de outros sistemas com os quais os recursos de informação são compartilhados; e

10) acesso à informação apenas ao seu proprietário, a outros indivíduos nominalmente autorizados ou a determinados grupos de usuários.

i) O monitoramento do uso e acesso ao sistema, com o objetivo de descobrir atividades não autorizadas, fornecendo evidências nos casos de incidentes de segurança, deve ser implementado.

Para isso, um registro (log) de eventos, com trilhas de auditoria registrando as exceções e outros aspectos de segurança relevantes, deve ser produzido e mantido por um período de tempo acordado para auxiliar em investigações futuras e no monitoramento do controle de acesso.

j) No mínimo, os registros (log) de auditoria incluem:

1) identificação dos usuários;

2) datas e horários de entrada (logon) e saída (logoff) no sistema;

3) identidade do terminal e, quando possível, a sua localização;

4) registros das tentativas de acesso ao sistema aceitas e rejeitadas; e

5) registros das tentativas de acesso a outros recursos e dados aceitas e rejeitadas.

k) Atenção especial deve ser dada à segurança dos registros de auditoria (log) porque, se adulterados, podem gerar uma falsa sensação de segurança.

l) Devem ser implementados controles que impeçam modificações não

autorizadas e problemas operacionais, destacando-se:

1) desativação dos registros (log);

2) alterações dos tipos de mensagens que são gravadas;

3) arquivos de registros (logs) sendo editados ou excluídos; e

4) esgotamento do meio magnético do arquivo de registros (logs), falhas no registro de eventos ou sobreposição do próprio arquivo.

m) Sistemas disponíveis publicamente.

1) É necessário proteger a integridade da informação divulgada eletronicamente, de forma a prevenir modificações não autorizadas que possam afetar a imagem do TCE/Am.

2) A divulgação de informações em sistemas de acesso público, como as existentes em um servidor acessível por meio da internet, necessita estar em conformidade com a legislação vigente.

3) Deve existir um processo de autorização formal, antes da publicação de uma informação.

4) É necessário que os arquivos de programas, dados e outras informações que requeiram alto nível de integridade, expostos em um sistema público, sejam protegidos por um método criptográfico que permita identificar se o arquivo sofreu algum tipo de alteração.

5) Sistemas de publicação eletrônica, especialmente aqueles que permitam retorno (feedback) e entrada direta de informações, são cuidadosamente controlados, de forma que:

a) a informação seja obtida em conformidade com a legislação relacionada à proteção de dados;

b) a entrada e o processamento de dados sejam feitos de forma completa e no devido tempo;

c) as informações sensíveis sejam protegidas, durante o processo de coleta e quando armazenadas; e

d) a forma de acesso a sistemas que divulguem informações não permita o acesso casual às redes nas quais esses sistemas estejam conectados.

6) Cuidados no uso da senha:

a) evitar anotação da senha em papéis, agendas e lembretes;

b) não salvar no computador (opção “lembrar senha”);

c) mudar periodicamente;

d) não escolher senhas óbvias;

e) não utilizar palavras contidas no dicionário de qualquer língua;

f) não repetir senhas já utilizadas;

g) evitar que novas senhas tenham trechos da anterior;

h) utilizar senhas que possam ser memorizadas e não anotadas;

i) usar senhas diferentes para máquinas diferentes;

j) tomar cuidado com ataques da engenharia social;

k) não emprestar senhas para outros usuários;

l) não utilizar senhas que possam ser facilmente ligadas ao usuário;

m) não informar a senha por e-mail ou por ligação telefônica;

n) não permitir que outrem observe quando a senha estiver sendo digitada;

o) utilizar senha forte com no mínimo 12 (doze) caracteres (algarismos, minúsculas, maiúsculas e caracteres especiais);

p) evitar utilizar, como senha, informações pessoais, nomes próprios ou combinações sequenciais do teclado (exemplo: asdfg); e

q) certificar-se de que cada usuário tenha uma conta individual com senha particular;

r) os sistemas em uso só habilitem o acesso mediante o uso de senha forte;

s) o arquivo de senhas só possa estar disponível para o administrador; e

t) haja troca de senhas forçada pelos sistemas, em intervalos regulares.

2.29 Medidas de segurança de conteúdo da informação nos MTIC

2.30 a) Criptografia:

1) é uma técnica utilizada para tornar ininteligível o texto da mensagem, mediante o emprego de cifras e chaves apoiadas em um algoritmo de transformação;

2) a qualidade do algoritmo criptográfico e o tamanho das chaves criptográficas a serem utilizadas são avaliados levando-se em conta o nível de proteção necessário;

3) quando as normas de criptografia no órgão são implementadas, é necessário atentar para as regulamentações e restrições nacionais que possam ter implicações nas técnicas criptográficas utilizadas em diferentes partes do mundo e com o fluxo de informações criptografadas além das fronteiras;

4) a criptografia pode ser de chave simétrica, que utiliza uma mesma chave tanto para codificar como para decodificar informações, ou de chave assimétrica - também conhecida como de chave pública - que utiliza duas chaves distintas, sendo uma pública, que pode ser livremente divulgada, e uma privada, que é mantida em segredo pelo seu proprietário;

5) o uso de sistemas criptográficos de origem estrangeira deve ser evitado, buscando-se o desenvolvimento e a adoção de tecnologia nacional, respeitada a necessidade de interoperabilidade com os sistemas adotados nos demais órgãos de controle externo, quando pertinente; e

2.31 b) Autenticação de mensagem:

1) é uma técnica utilizada para garantir a integridade de mensagens enviadas, detectando modificações não autorizadas ou corrupção do seu conteúdo.

2) diferentemente da criptografia, essa técnica não é projetada para proteger o conteúdo da mensagem de divulgação não autorizada.

2.32 c) Assinatura digital:

1) fornece o meio para proteção da autenticidade, integridade e não repúdio de documentos eletrônicos;

2) é aplicada a qualquer forma de documento processado digitalmente;

3) implica considerar o tipo e a qualidade do algoritmo usado e o tamanho da chave; e

4) impõe que as chaves criptográficas utilizadas sejam diferentes das usadas para criptografia.

2.33 d) Serviços de irretratabilidade (não repúdio):

1) são usados nos casos em que seja necessário resolver disputas sobre ocorrência ou não de um evento ou ação;

2) visam a garantir que o autor não negue ter executado a ação como, por exemplo, criar, enviar ou assinar digitalmente um documento; e

3) são baseados no uso de criptografia e técnicas de assinatura digital.

2.34 e) Outras técnicas – A aplicação conjunta das técnicas que foram expostas, ou o emprego de outras técnicas, pode ser implementada com o objetivo de buscar maior segurança do conteúdo.

2.35 Medidas de segurança de transmissão da informação nos MTIC

a) Essas medidas visam a proteger fisicamente os meios de comunicações, a dificultar a interceptação de mensagens e a consequente análise do seu fluxo.

b) Todo o tipo de serviço corporativo de redes de comunicações, seja no contexto local ou remoto, deve contemplar:

1) processos de gerenciamento capazes de monitorar e registrar os eventos relativos ao funcionamento dos referidos serviços, de forma a permitir que o fiel cumprimento das regras de Segurança da Informação nos MTIC seja verificado, a partir de autorização pelo escalão superior ou por órgão competente, quando for o caso;

2) procedimentos de manutenção dos referidos serviços;

3) mecanismos de defesa contra ataques aos referidos sistemas;

4) procedimentos para aferir a efetividade das ações adotadas, tanto periódicas quanto inopinadas; e

5) medidas de contingência em condições de ativação imediata.

2.36 c) Medidas a serem executadas:

2.37 1) esteganografia – método usado para tornar a mensagem imperceptível aos sentidos humanos, mediante o emprego de técnicas específicas. A diferença entre esteganografia e criptografia é que, enquanto esta visa a esconder o conteúdo das mensagens, aquela objetiva esconder a sua existência.

Se imaginarmos que um ataque bem-sucedido à criptografia consiste em decodificar uma mensagem cifrada, um ataque bem-sucedido à esteganografia consiste em detectar a mensagem escondida;

2) escolha dos locais para instalação dos equipamentos – como primeira providência, impõe-se a necessidade de serem escolhidos os locais para instalação dos equipamentos de TIC.

Essa medida visa a criar obstáculos às ações de interceptação; em particular, àquelas voltadas para as linhas que configuram o esquema dos meios de telecomunicações (telefones fixos e móveis, cabos de rede e cabos de fibra ótica, entre outros).

Os locais escolhidos são avaliados em razão do fluxo de pessoas, que pode impactar no aumento do risco de ações de espionagem e sabotagem;

3) escolha do meio de comunicações – o meio de comunicações a ser empregado deve ser selecionado de acordo com a sensibilidade da informação a ser transmitida.

A perfeita adequação é obtida pelo justo equilíbrio entre os princípios da oportunidade e da segurança. Na escolha do meio a ser empregado, é considerado o aspecto da alternância, buscando-se variações constantes, seja dos equipamentos, operadores ou mensageiros;

4) exploração adequada dos meios de comunicações – essa medida, ligada à anterior, tem por objetivo estabelecer não só os procedimentos que permitam o uso correto dos meios, mas também a disciplina na exploração. Deve ser determinado quem pode transmitir o quê, por quais meios e em que momento;

5) utilização do código de chamada – objetiva estabelecer os procedimentos relativos à exploração de um sistema de sinais convencionados, que confirme ao receptador a real origem da chamada (autenticidade). Visa também, em última análise, a dificultar ações hostis de intromissão na rede de comunicações;

6) exploração do tráfego falso – a utilização de falsas mensagens permite iludir ou confundir o interceptador quanto ao volume e à intensidade do fluxo de mensagens transmitidas, ao mesmo tempo em que pode oferecer ao adversário informação adulterada intencionalmente, neutralizando as ações hostis de busca. Requer planejamento detalhado e execução centralizada.

2.38 Segurança dos sistemas de automação de documentos

a) Esses sistemas favorecem a rápida disseminação e compartilhamento de informações, utilizando-se de uma combinação de documentos, computadores, computação móvel, comunicação móvel, correio eletrônico, correio de voz, comunicação de voz em geral, multimídia, serviços postais e máquinas de fax.

b) As considerações relacionadas à segurança do órgão, que estão en-

volvidas com esse conjunto de recursos, incluem:

1) uso de rede segregada;

2) exclusão das informações sensíveis, caso o sistema não forneça o nível de proteção apropriado;

3) especificar os servidores, prestadores de serviço ou terceiros autorizados a usarem os sistemas, além dos locais a partir dos quais eles possam ser acessados;

4) restrição de facilidades selecionadas a categorias específicas de usuários;

5) identificação da categoria dos usuários, como, por exemplo, listas dos servidores do órgão ou prestadores de serviço, em benefício de outros usuários;

6) geração e retenção de arquivos cópias de informação mantidos no sistema; e

7) requisitos e acordos de recuperação e contingência.

2.39 Segurança de redes de computadores

a) As páginas eletrônicas (home pages) devem estar de acordo com o padrão utilizado para Elaboração de Páginas Eletrônicas dos demais TCs, e hospedadas nos domínios disponibilizados pelo TCE/AM.

b) Os computadores que estiverem conectados à internet, ou a outras redes com acesso remoto, não devem conter informação sensível.

c) Toda rede, conectada à internet ou não, deve possuir ferramentas atualizadas, capazes de:

1) identificar ou dificultar o acesso de pessoas não autorizadas; e

2) rastrear e emitir relatórios sobre os pontos vulneráveis que podem ser utilizados como porta de entrada para a invasão nos sistemas.

d) A pasta “público” ou similar, normalmente disponível em redes do órgão, não deve ser utilizada para armazenamento de arquivo que contenha informação sensível.

2.40 Segurança no correio eletrônico

a) O uso de correio-eletrônico (e-mail) com contas oficiais e funcionais sob domínio do TCE/AM é exclusivo para tramitação de assuntos profissionais. Essa ferramenta somente pode ser utilizada para o envio de mensagens contendo informação sensível, se for utilizado um sistema criptográfico.

b) E-mail particular, que não esteja sob domínio do TCE/AM, não deve ser utilizado para assuntos profissionais.

c) Os e-mails recebidos de procedência desconhecida não devem ser abertos, principalmente os que contenham arquivos anexados.

d) O envio de mensagens por meio de correios eletrônicos não corporativos pode comprometer a segurança da informação.

2.41 Trabalho remoto

a) O trabalho remoto utiliza tecnologia de comunicação para permitir que usuários trabalhem de uma localização física fora do órgão.

b) É necessário implantar a proteção apropriada do local do trabalho remoto para evitar, por exemplo, o roubo do equipamento e de informações, a divulgação não autorizada de informação, o acesso remoto não autorizado aos sistemas internos do órgão ou o uso impróprio desses recursos.

c) São considerados os seguintes aspectos para utilização de trabalho remoto:

1) a segurança física existente no local;

2) a adequação do ambiente para realização do trabalho remoto;

3) os requisitos de segurança nas comunicações; e

4) o risco de acesso não autorizado à informação por outras pessoas que utilizam o local e não tenham necessidade de conhecer.

e) Os controles e providências que são considerados incluem:

1) a provisão de equipamento e mobília apropriados às atividades de trabalho remoto

2) a definição do trabalho permitido, as horas de trabalho, a classificação da informação que pode ser tratada e os sistemas internos e serviços cujo acesso será autorizado;

3) a provisão de equipamento de comunicação apropriado, incluindo métodos para acesso remoto seguro;

4) a segurança física;

5) as regras e orientações sobre o acesso de familiares e visitantes ao equipamento e à informação;

6) a provisão de suporte e manutenção de equipamento e software;

7) os procedimentos para cópias de segurança e continuidade do serviço;

8) auditoria e monitoramento da segurança; e

9) revogação de autoridade, direitos de acesso e devolução do equipamento quando as atividades de trabalho remoto não forem mais necessárias.

2.42 Procedimentos de Backup

a) Com o objetivo de se manter a integridade e a disponibilidade dos serviços de comunicação e processamento da informação, é necessário estabelecer procedimentos para a execução das cópias de arquivos e para a disponibilização dos recursos de reserva.

b) Esses procedimentos são discriminados nas medidas de contingência, de forma a viabilizar a restauração de dados e informações com oportunidade, bem como controlar e registrar eventos e falhas.

2.43 Auditorias e Tratamento de Incidentes

a) Medidas recomendadas:

1) identificação e registro das modificações significativas;

2) análise de impacto potencial de tais mudanças;

3) procedimento formal de aprovação das mudanças propostas;

4) comunicação dos detalhes das modificações para todas as pessoas com envolvimento relevante; e

5) procedimentos que identifiquem os responsáveis para a suspensão e recuperação de mudanças no caso de insucesso.

b) É necessário que as responsabilidades e procedimentos de gerenciamento de incidentes sejam definidos para garantir respostas rápidas, efetivas e ordenadas aos incidentes de segurança.

c) São estabelecidos procedimentos relativos a todos os tipos potenciais de incidentes de segurança, incluindo:

1) falhas dos sistemas de informação e inoperância de serviços;

2) negação de serviço;

3) erros resultantes de dados incompletos ou inconsistentes; e

4) violação de grau de sigilo.

2.44 Medidas de Segurança da Informação em mídias sociais e em aplicativos de TI

a) É proibida a difusão de informações sensíveis por aplicativos de mensagem instantânea, mídias sociais e redes de relacionamento.

b) Evitar o uso de mídias sociais e de aplicativos desconhecidos que possam conter funções como geolocalização e compartilhamento de informações pessoais.

c) O uso de mídias sociais, por servidores que operem com informações sensíveis, deve estar em consonância com as regras estabelecidas pela Instituição.

2.45 Medidas de Segurança da Informação nos aparelhos de telefonia celular

a) Aparelhos celulares são repositórios de dados e informações. Documentos de serviço, de qualquer natureza, não devem ser arquivados nesses aparelhos, que podem ser extraviados, furtados ou roubados, causando o comprometimento dos dados neles arquivados.

b) Especial atenção deve ser dada a conversas arquivadas em aplicativos de comunicação instantânea e similares. Assuntos de serviço não devem ser tratados por intermédio desse tipo de recurso.

2.46 Segurança da Informação nas Áreas e Instalações

A Segurança da Informação, nas Áreas e Instalações, consiste no subgrupo de medidas voltadas para preservar as informações sobre áreas e instalações pertencentes ou de interesse do TCE/AM.

Ações hostis contra áreas e instalações podem ser executadas pelo uso de meios cibernéticos, óticos ou eletrônicos, dentre outros. Por conseguinte, impõe-se a avaliação da existência de informações nas áreas e instalações, que possam ser exploradas pelas ameaças, com o objetivo de definir “onde” e “o quê” será protegido. Como exemplo de Informações de Áreas e Instalações a serem protegidas, destacam-se as vistas aéreas, plantas, maquetes e fotografias internas, contidas em arquivos digitais ou físicos, que indiquem os locais do órgão sob restrição de acesso.

A fim de diminuir os riscos concernentes à Segurança da Informação nas Áreas e Instalações, uma medida adequada é não permitir a entrada de pessoas portando equipamentos de comunicação, filmagem ou geração de imagens

em áreas e instalações que necessitem ser protegidas. Cuidados especiais devem ser tomados diante da miniaturização desses equipamentos.

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (TCMS)

Nome, nacionalidade, CPF, RG (nº, data e local de expedição), (filiação e endereço), estado civil (se casado/a ou com união estável identificar o parceiro/a), e-mail funcional, perante o Tribunal de Contas do Estado do Amazonas (TCE/AM), declaro ter ciência inequívoca da legislação sobre o tratamento de informações sensíveis e classificadas cuja divulgação possa causar risco ou dano à segurança do TCE/AM, à sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527/2011, dispositivos do Estatuto dos Servidores Estaduais do Amazonas e Código Penal Brasileiro, e a:

a) tratar as informações sensíveis e classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo TCE/AM e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;

c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

d) não copiar ou reproduzir, por qualquer meio ou modo:

(i) informações sensíveis e classificadas em qualquer grau de sigilo; e

(ii) informações relativas aos materiais de acesso restrito do TCE/AM, salvo por meio de autorização da autoridade competente.

Declaro que por estar de acordo com o presente Termo, o assino na presença das testemunhas abaixo identificadas.

Local de data

Assinatura

Testemunha identificada 1

Testemunha identificada 2

APÊNDICE 1

SUGESTÕES SOBRE SEGURANÇA ORGÂNICA

1. Não deposite na cesta de papéis: rascunhos e cópias contendo dados ou informações sensíveis.

2. Retire de sua mesa de trabalho, antes de deixar a sala, documentos que não devem ficar expostos, guardando-os em local apropriado. Ao término do expediente, verifique se os arquivos, gavetas e portas de armários estão fechados e trancados.

3. Assunto sigiloso não se trata por telefone. Não há segurança neste meio de comunicação.

4. A sua condição ou suas atribuições de serviço não deverão ser objeto de conversas em reuniões sociais, bares, restaurantes, coletivos etc.

5. Tenha em mente que, em reuniões sociais, você não sabe quem está escutando.

6. No serviço, não procure inteirar-se de assuntos que não sejam de suas atribuições ou não estejam sob sua responsabilidade. Respeite a necessidade de conhecer.

7. Informações sobre documentos somente deverão ser fornecidas a quem estiver devidamente credenciado e tiver necessidade de conhecer.

8. Lembre-se de que a necessidade de conhecer dados e informações sigilosas depende da função desempenhada e não do seu grau hierárquico.

9. Qualquer indício de risco para a segurança dos recursos humanos, das informações, do material e das áreas e instalações deve ser imediatamente comunicado ao membro do CGSI.

10. Colabore com a Guarda. Seja militar ou empresa de segurança terceirizada. Eles estão ajudando a cumprir as normas de segurança.

APÊNDICE 2

PROCEDIMENTOS DE MESAS E TELAS LIMPAS

1. O órgão deve considerar a adoção de procedimentos de mesas de trabalho limpas para papéis e mídias removíveis e de telas de monitores de meios informatizados limpa, de forma a reduzir riscos de acesso não autorizado, perdas e danos à informação.

2. Os procedimentos devem levar em consideração as classificações da segurança da informação, os riscos correspondentes e os aspectos culturais do órgão.

3. As informações deixadas em mesas de trabalho são alvos prováveis de danos ou destruição em eventos tais como incêndio, inundações ou explosões.

4. Recomenda-se que, entre outros, os seguintes controles sejam considerados:

a) onde e quando apropriado, é necessário que papéis e mídias sejam guardados de forma segura, em mobiliário adequado, durante os momentos em que não estiverem sendo utilizados;

b) computadores pessoais, terminais de computador e impressoras não devem ser deixados ligados sem a presença do usuário e devem ser protegidos por senhas, chaves ou outros controles quando não estiverem em uso;

c) pontos de recepção e envio de correspondências, sem a presença do usuário, devem ser protegidos;

d) copiadoras devem ser travadas (ou, de alguma forma, protegidas contra o uso não autorizado) fora do horário normal de trabalho; e

e) sempre que possível, o usuário deve usar senha para imprimir qualquer documento contendo dados ou informações sensíveis, os quais devem ser retirados da impressora imediatamente.

TERMOS E DEFINIÇÕES

Ameaça – conjunção de ator, motivação e capacidade de realizar ação hostil, real ou potencial, com possibilidade de, por intermédio da exploração de deficiências, comprometer as informações, afetar o material, o pessoal e seus valores, bem como as áreas e instalações, podendo causar danos.

Análise de Riscos – estabelecimento da probabilidade de o risco ocorrer e de seu impacto nos ativos da instituição.

Autenticação – declaração de que um documento original é autêntico, ou que uma cópia reproduz fielmente o original, feita por uma pessoa jurídica com autoridade para tal (servidor público, notário ou autoridade certificadora) em um determinado momento.

Autenticação de mensagem – técnica utilizada para garantir a integridade de mensagens enviadas, detectando modificações não autorizadas ou corrupção do seu conteúdo.

Avaliação de Riscos – interação entre a probabilidade e o impacto, estabelecendo-se o valor e o nível de risco, que tem por finalidade auxiliar na tomada de decisão para o tratamento de riscos.

Classificação – o ato de se atribuir grau de sigilo à informação que requeira medidas especiais de salvaguarda e, por consequência, aos seus suportes.

Compartimentação – restrição do acesso com base na necessidade de conhecer.

Confidencialidade (sigilo) – garantia de que o conteúdo da informação só é acessível e interpretável por quem possuir autorização para a ela ter acesso.

Comprometimento – perda de segurança resultante do acesso não autorizado.

Criptografia – técnica utilizada para tornar ininteligível o texto da mensagem, mediante o emprego de cifras e chaves apoiadas em um algoritmo de transformação.

Disponibilidade – garantia de que o conteúdo da informação esteja disponível para quem possuir autorização ou credencial de segurança, sempre que houver necessidade.

Espionagem – ação realizada por pessoal, vinculado ou não a serviço de Inteligência, visando à obtenção de conhecimento, dado sigiloso, documento ou material para beneficiar Estados, grupos de países, organizações, facções,

empresas, personalidades ou indivíduos.

Informação classificada – informação sigilosa em poder do órgão ou entidade pública, que recebeu de autoridade competente classificação no grau de sigilo ultrassecreto, secreto ou reservado devido ao seu teor, e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado.

Informação de acesso restrito – informação que, desclassificada ou não sendo passível de receber classificação sigilosa, por sua utilização ou finalidade, demanda medidas especiais de proteção.

Informação sensível – informação classificada, de acesso restrito ou ostensiva que, em decorrência de sua natureza ou conteúdo, necessite de medidas de proteção.

Informação sigilosa – informação submetida, temporariamente, à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado ou por ser abrangida pelas demais hipóteses legais de sigilo.

Integridade – garantia de que o conteúdo original da informação não seja modificado; é a certeza de que a exatidão e a inteireza estejam salvaguardadas.

Irretratabilidade (não repúdio) – garantia de que, num processo de envio e recebimento de informações, qualquer participante originador ou destinatário de informação não possa, em um momento posterior, negar a respectiva atuação.

Malwares – programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Eles podem ser vírus, worm, bot, spyware, backdoor, cavalo de troia (trojan horse), rootkite ransomware, entre outros.

Medidas de Contingência – medidas estabelecidas com o objetivo de prover meios e procedimentos alternativos, diante de situações que ameacem a Segurança Orgânica, com o intuito de assegurar a continuidade ou restabelecer o funcionamento dos ativos afetados.

Necessidade de conhecer – condição pessoal, inerente ao efetivo exercício de cargo, da função, do emprego ou da atividade, indispensável para que uma pessoa tenha acesso à informação sensível.

Phishing – e-mails que parecem ser enviados por pessoas conhecidas ou por organizações legítimas, normalmente visando a induzir o usuário a clicar em um arquivo malicioso anexado ou direcioná-lo a um site falso, também malicioso.

Plano de Controle de Danos – plano composto de medidas que devem ser adotadas para verificar, em caso de dano, o comprometimento dos ativos que deveriam ter sido protegidos e suas consequências.

Ransomware – tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

Rootkit – conjunto de programas e técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido, impedindo sua detecção pelo usuário e por mecanismos de segurança.

Sabotagem – qualquer ação sub-reptícia destinada a perturbar, interferir, causar dano, destruir ou comprometer o funcionamento normal de diferentes sistemas nos campos político, econômico, científico-tecnológico, psicossocial e militar.

Segurança da Informação – grupo de medidas destinado a garantir a disponibilidade, integridade, confidencialidade (sigilo), autenticidade, a irretratabilidade (não repúdio) e atualidade da informação em todo o seu ciclo de vida.

Spyware – programa projetado para monitorar as atividades de um sistema, coletando hábitos online, histórico de navegação ou informações pessoais (como senhas, por exemplo), enviando as informações coletadas para terceiros.

Vírus – programas que se propagam inserindo cópias de si mesmos, tornando-se parte de outros programas e arquivos.

Vazamento – divulgação não autorizada de informação sensível.

Vulnerabilidade – deficiência que, ao ser explorada pela ameaça, pode causar incidentes de segurança e gerar impactos negativos para o Exército Brasileiro.

Worm – programa que envia cópias de si mesmo de computador para computador. Diferentemente do vírus, o worm não precisa ser executado pelo usuário, propagando-se pela execução automática de suas cópias e explorando deficiências existentes em programas instalados nos computadores.