MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
BATALHÃO DE POLÍCIA DO EXÉRCITO DE BRASÍLIA
(6ª Cia Gd/1957)
BATALHÃO BRASÍLIA

Aditamento Nr 003 - 1ª Seção/BPEB ao Boletim Interno Nr 108

Quartel Brasília, Distrito Federal.

Em 08 JUN 17 (5ª Feira)

Para conhecimento deste Batalhão e devida execução, publico o seguinte:

1ª Parte

SERVIÇOS DIÁRIOS

Sem alteração.

2ª Parte

INSTRUÇÃO

Sem alteração.

3ª Parte

ASSUNTOS GERAIS E ADMINISTRATIVOS

1. **ALTERAÇÕES DE OFICIAIS**

Sem alteração.

2. **ALTERAÇÕES DE SUBTENENTES E SARGENTOS**

Sem alteração.

3. **ALTERAÇÕES DE CABOS E SOLDADOS**

Sem alteração.

4. **DIVERSOS**

Política de Segurança da Informação e Comunicações/BPEB - Publicação

1. Finalidade

Art. 1º. Este documento tem por finalidade estabelecer Diretrizes de Segurança da Informação e Comunicações a serem adotadas pelos integrantes do BATALHÃO DE POLÍCIA DO EXÉRCITO DE BRASILIA (BPEB), de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação armazenada ou em trânsito nos sistemas computacionais desta Organização Militar.

Art. 2º. Constituem propósitos destas Diretrizes:

I – formalizar direitos e responsabilidades de usuários, administradores de redes e sistemas e especialistas em segurança da informação do BPEB;

II – garantir o bom uso dos recursos de Tecnologia da Informação e Comunicações (TIC);

III – atribuir papéis e responsabilidades na elevação dos níveis de segurança da informação no âmbito do BPEB;

IV – disseminar a cultura de segurança da informação no âmbito do BPEB.

2. Objetivos

Art. 3º. São objetivos desta Política:

I – definir e estabelecer procedimentos relacionados à Segurança da Informação e Comunicações a serem adotados pelos integrantes do BPEB;

II – normatizar, no âmbito do BPEB, o uso dos recursos de TIC;

III – estabelecer regras para o controle de acesso aos recursos de TIC e à Rede Mundial de Computadores a partir da rede local do BPEB;

IV – atribuir papeis e responsabilidades na utilização, operação e manuseio dos recursos computacionais do BPEB.

3. Conceitos e Pressupostos Básicos

Art. 4º. Compreende-se como recurso de TIC, para os efeitos desta Política, todo e qualquer dispositivo eletrônico que possibilite a transmissão, o armazenamento e a reprodução de voz e dados em equipamento isolado ou em rede, além do conhecimento técnico do pessoal especializado que viabiliza o fluxo da informação pelos canais de comunicações, mediante o emprego da tecnologia disponível.

Art. 5º. Entende-se por dispositivo móvel qualquer tipo de notebook, tablet, smartphone, telefone celular ou equipamentos similares a estes.

Art. 6º. Os dispositivos de TI incluídos no patrimônio do BPEB são colocados à disposição dos seus militares para uso exclusivo em atividades estritamente relacionadas às funções institucionais por eles desempenhadas.

Art. 7º. Considera-se como matéria ilícita: pornografia e erotismo; qualquer forma de discriminação, seja ela étnica, religiosa, ideológica, política ou de orientação sexual; assuntos contrários à ética, à disciplina militar, à moral e aos bons costumes, bem como atentatória à ordem pública ou que viole qualquer direito de terceiros conforme definido na Constituição Federal, em Leis, em Decretos ou em Regulamentos.

Art. 8º. A fim de facilitar a compreensão deste documento e elucidar conceitos, as seguintes definições são necessárias:

I – ameaças: condições que podem causar incidentes por meio da descoberta de vulnerabilidades;

II – antivírus: programa que detecta e anula ou remove malwares de um computador;

III – ativo: a informação em si ou qu que a que lquer componente que compõe os processos e interfere direta ou indiretamente no fluxo de informação na instituição desde sua origem até seu destino, tais como equipamentos computacionais, sistemas, manuais, ferramentas e mídias;

IV – backup: cópia de segurança ou meio de armazenamento secundário que contém uma reprodução da informação de arquivos ou conjunto de dados;

V – correio eletrônico (e-mail): ferramenta que possibilita a transferência de mensagens e qualquer outro documento eletrônico para fins de comunicação;

VI – cookie: arquivo com informações que os sítios de Internet, ao serem visitados, podem armazenar nos navegadores (browsers) de forma que, na próxima visita ao mesmo endereço, este já possua informações úteis sobre o usuário;

VII – dispositivo de armazenamento: dispositivo físico no qual se registram informações para recuperação futura, podendo ser fixo ou removível (HD, CD, DVD, pen drive, fita, disquete, cartão de memória flash, entre outros);

VIII – estação de trabalho: computador com recursos voltados para a produtividade pessoal e que completa suas necessidades com recursos de outros computadores na rede;

IX – firewalls: dispositivos constituídos pela combinação de software e hardware, utilizados para dividir e controlar o acesso a computadores (firewall pessoal) ou redes (firewall de rede), separando um ambiente seguro de um ambiente de rede hostil;

X – hardware: é o conjunto de elementos de um sistema computacional formado pelos componentes eletrônicos e partes físicas, como por exemplo monitores, processadores, teclados, discos rígidos, placas e qualquer outro material que seja necessário ao funcionamento de um equipamento de TI;

XI – hardening: é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas. Em geral, o processo inclui remover ou desabilitar nomes ou logins de usuários que não estejam mais em uso ou não são mais necessários, desabilitar serviços desnecessários e atualizar softwares;

XII – informação: principal ativo das corporações e que requer grande proteção, de acordo com o seu valor para a organização;

XIII – informação sensível: toda e qualquer informação que quando utilizada de maneira inadequada pode causar prejuízos financeiros, material ou à imagem de pessoas ou

instituições. Exemplos de informações sensíveis são: número de protocolo de documentos, endereços de funcionários. Detalhes sobre topologia de redes, configurações técnicas de ativos, rotinas e procedimentos internos da Organização, entre outros;

XIV – log: registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

XV – NTP (Network Time Protocol): protocolo para sincronização dos relógios dos sistemas computacionais

XVI – risco: probabilidade de exploração das vulnerabilidades pelas ameaças, causando impacto na organização;

XVII – software: componente lógico e intangível de um computador, que engloba arquivos executáveis, bibliotecas, programas e sistemas operacionais;

XVIII – usuários internos: militares integrantes do BPEB ou civis autorizados que se encontrem prestando serviço para o BPEB;

XIX – usuários externos: todos os usuários de organizações externas que, direta ou indiretamente, acessam os recursos de TIC disponibilizados pelo BPEB, incluindo-se os empregados de empresas prestadoras de serviços terceirizados e consultores autorizados a utilizar em caráter temporário os recursos tecnológicos do BPEB;

XIX – malware: software desenvolvido e empregado com o objetivo de executar operações maliciosas nos computadores em que se instala, como corrupção de dados, roubo de informações, envio de mensagens de spam e ataques contra outros servidores.

4. Referências

Art. 9º. São referências para este documento:

I – Constituição da República Federativa do Brasil – 1988;

II – Lei n° 9.296, de 24 de julho de 1996 – Regulamenta o inciso XII, parte final, do Art 5° da Constituição Federal, sobre a interceptação de comunicações telefônicas;

III – Lei 12.737, de 30 de novembro de 2012;

IV – Norma Complementar Nr 03/IN01/DSIC/GSIPR – Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

V – Decreto-Lei N° 1.001, de 21 de outubro de 1969 – Código Penal Militar;

VI – Decreto no 4.346, de 26 de agosto de 2002 – Regulamento Disciplinar do Exército (R-4);

VII – Decreto No 7.845, de 14 de novembro de 2012;

VIII – Portaria N° 049-DCT, de 19 de dezembro de 2005 – Aprova as Instruções Reguladoras para Emprego Sistêmico do Serviço de Correio Eletrônico no Exército Brasileiro – IRESCE (IR 13-06);

IX – Portaria N° 026-DCT, de 31 de março de 2006 – Aprova as Instruções Reguladoras para Emprego Sistêmico da Informática no Exército Brasileiro (IR 13-07);

X – Portaria N° 003-DCT, de 31 de janeiro de 2007 – Aprova as Instruções Reguladoras sobre Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro – IRASEG (IR 13-09);

XI – Portaria N° 004-DCT, de 31 de janeiro de 2007 – Aprova as Instruções Reguladoras sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro – IRESER (IR 13-15);

XII – Portaria N° 006-DCT, de 5 de fevereiro de 2007 – Aprova as Normas para Controle da Utilização dos Meios de Tecnologia da Informação no Exército – NORTI (2a Edição);

XIII – Portaria N° 011-DCT, de 29 de março de 2010 – Aprova o Plano de Migração para Software Livre no Exército Brasileiro, versão 2010;

XIV – Portaria N° 720-Cmt Ex, de 21 de novembro de 2011 – Aprova a Cartilha Emergencial de Segurança da Tecnologia da Informação e Comunicações (Versão 1.0);

XV – Of No 573 – A2.C/DCT – CIRCULAR, de 13 de novembro de 2009;

XVI – DIEx no 2-SEC INTLG/DCT, de 21 de janeiro de 2014.

XVII – Portaria No 1.067, de 8 de setembro de 2014 – Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), 1a Edição, 2014.

5. Regras de Segurança

Art. 10. São regras gerais:

I – todos os integrantes do BPEB são responsáveis pela elevação dos níveis de segurança da informação no âmbito desta OM;

II – todo militar usuário dos recursos de TIC do BPEB deverá assinar o Termo de Compromisso e Manutenção de Sigilo, conforme modelo do Anexo A;

III – todo militar do BPEB que for usuário dos recursos de TIC deverá ter o exato conhecimento destas regras;

IV – será adotado no âmbito do BPEB, para o direito de acesso aos recursos de TIC, o princípio do privilégio mínimo, ou seja, o usuário só terá privilégio para acesso ao que for estritamente necessário ao desempenho de suas funções;

V – a impressão de documento, nas impressoras disponibilizadas pelo BPEB, é de inteira responsabilidade do dono do documento, devendo este zelar para que cópias ou rascunhos sem o devido controle não estejam disponíveis nas impressoras do BPEB;

VI – todo documento inservível que contenha informações sensíveis deverá ser encaminhado à Seção de Inteligência para ser picotado e descartado em lixeira adequada;

VII – será adotada no BPEB a política de mesa e tela limpa, ou seja, os usuários dos recursos de TIC do BPEB não deverão deixar desnecessariamente documentos, classificados ou não, sobre a mesa. Os usuários deverão ainda providenciar para que ao se ausentar de sua estação de trabalho a mesma tenha sua tela bloqueada, impedindo assim o acesso à sua área de trabalho;

VIII – toda informação produzida, manuseada ou arquivada no BPEB deverá passar por uma avaliação crítica quanto à classificação sigilosa;

IX – o Sistema de Protocolo Eletrônico de Documentos (SPED) somente deverá ser utilizado para a produção de documentos de caráter ostensivo;

X – o protocolo, o envio e o arquivamento de documentos com classificação sigilosa será realizado pela Seção de Inteligência;

XI – todos os documentos sigilosos deverão ser protocolados, mesmo os de natureza interna;

XII – poderá ser utilizado o serviço de correio eletrônico corporativo para troca de informações profissionais diversas, desde que essas não requeiram classificação sigilosa. Contudo, quando for necessária a formalização de determinada informação, essa deverá ser feita via produção de documento no SPED;

XIII – é terminantemente proibido o armazenamento de arquivos e dados atinentes ao serviço em sistemas virtuais externos ao ambiente da EBNet tais como Google Drive, Dropbox, iCloud, Ubuntu One;

XIV – caso seja necessária a utilização de serviço de armazenamento em nuvem, os militares do BPEB poderão utilizar a solução disponibilizada pelo BPEB. Contudo, apenas documentos de natureza ostensiva poderão ser armazenados em tal serviço;

XV – a Seção de Informática deverá trabalhar preventivamente na otimização da segurança da informação no âmbito deste aquartelamento. Esse trabalho, além do operacional, deverá ocorrer através do processo de conscientização do público interno, seja este por meio de campanhas de divulgação de novas ameaças, instruções, workshops ou qualquer outro meio que leve ao aumento da eficiência dos processos de segurança da informação e comunicações;

XVI – todo servidor ou estação de trabalho da rede interna deverá ter sua data e hora sincronizada como o serviço NTP do Sistema de Telemática do Exército (ntp.eb.mil.br), devendo a Seção de Informática providenciar a sincronização das estações de trabalho e a Divisão de Operação a sincronização nos servidores da rede interna;

Art. 11. Da formação e uso de senhas:

I – o credenciamento para acesso aos sistemas utilizados no âmbito deste Batalhão será feito mediante cadastro de usuário e senha, conhecimento desta Política e assinatura do Termo de Compromisso e Manutenção de Sigilo;

II – ao escolher sua senha o usuário requerente deverá observar os requisitos de formação de uma senha robusta, ou seja, este deverá formar sua senha mesclando letras maiúsculas e minúsculas, números e símbolos especiais, além de ter um tamanho mínimo de oito caracteres;

III – é proibido o compartilhamento de usuário e senha para acesso a qualquer sistema existente ou utilizado neste Centro.

Art. 12. Da utilização de dispositivos móveis:

I – é expressamente proibida a utilização de dispositivos móveis pessoais na rede de dados do BPEB;

II – o compartilhamento de arquivos no âmbito do BPEB deverá ocorrer utilizando-se os serviços fornecidos pelo Batalhão (servidor de arquivos, servidor FTP), sendo proibida a utilização de pen drives e HDs externos pessoais ou quaisquer dispositivos similares a estes;

III – poderá ser utilizado, para trâmite de arquivos entre o BPEB e órgãos externos, apenas dispositivos móveis institucionais. Esse uso, contudo, deve ser evitado e caso seja necessário, o dispositivo deverá ser criptografado, preferencialmente utilizando a solução padronizada pele 7º CTA;

IV – notebooks institucionais deverão ter seus discos rígidos criptografados;

V – notebooks institucionais deverão ser configurados para não armazenarem cookies e históricos em seus navegadores;

VI – notebooks institucionais deverão possuir contas sem privilégios para tantos usuários comuns quanto forem necessários, devendo a utilização da conta de administrador à Seção de Informática para a administração do sistema operacional.

Art. 13. Da segurança do hardware:

I – todo material de TI de uso permanente deverá constar no Sistema de Controle Físico – Módulo OM (SISCOFISOM), devendo existir em cada seção um inventário atualizado do material a ela distribuído, bem como o nome do detentor indireto deste;

II – deverá haver trimestralmente a conferência do material existente nas seções do BPEB, devendo as alterações serem informadas de forma documentada à Divisão Administrativa;

III – o material de TI destinado a consumo deverá ser controlado, ficando a cargo da Seção de Informática;

IV – todo material de TI retirado do aquartelamento, sob cautela, deverá estar autorizado pelo Fiscal Administrativo da OM a qual o material pertença, devendo ser preenchido o formulário de Autorização de Retirada de Material de TI, constante no Anexo C. Este formulário deverá permanecer com o detentor indireto da carga da qual o material foi retirado;

V – microcomputadores pertencentes ao parque computacional do BPEB deverão estar lacrados e com seus componentes e acessórios controlados por meio do Open Computer and Software Inventory (OCS Inventory);

VI – ativos de rede deverão ser acondicionados em armários chaveados, de forma a impedir o livre acesso a ele, exceção feita aos ativos localizados no data center;

VII – é proibida a mudança da disposição dos ativos de TI sem a devida autorização do Chefe da Seção de Informática e dos chefes de seção/comandantes envolvidos e sem a realização prévia de uma análise de risco;

VIII – a Seção de Informática deverá controlar o processo de lacre e cadastramento no OCS Inventory dos microcomputadores do parque computacional do BPEB. Apenas a Seção de Informática, está autorizada a romper lacre e substituir acessórios ou componentes dos microcomputadores do BPEB.

Art. 14. Da segurança do software:

I – fica padronizado para utilização no âmbito da rede interna, o sistema operacional GNU/Linux do BPEB, ficando as exceções restritas aos casos absolutamente necessários e sob a avaliação do Chefe da Seção de Informática;

II – sistemas operacionais que necessitam de antivírus devem utilizar a solução institucional configurada para ser atualizada automaticamente. Na ausência de uma solução institucional a ser adotada pelo BPEB, deverá ser utilizado o software Antivírus (kaspersky), conforme orientação do 7º CTA;

III – os antivírus instalados no parque computacional desta OM devem ser configurados para executarem automaticamente a varredura no sistema operacional e em mídias removíveis conectadas ou inseridas nos computadores ligados à rede interna;

IV – apenas a Seção de Informática tem a autorização para instalar, remover ou modificar sistemas operacionais instalados na rede interna deste Batalhão;

V – apenas a Seção de Informática deverá possuir senha de administrador (root) nos sistemas operacionais da rede interna e providenciar para que os usuários tenham acesso apenas como usuários comuns;

VI – não deverá haver compartilhamento de diretórios home. Contudo, caso haja necessidade de dois ou mais usuários compartilharem a mesma máquina, o acesso deve ser individualizado com a criação de quantas contas forem necessárias, sendo possível assim o rastreamento das ações de cada operador;

VIII – deverá ser executado o hardening básico dos sistemas operacionais para os usuários internos, atentando para que estes não percam funcionalidades básicas.

IX – a Seção de Informática deverá implementar mecanismo de descarte ou de alienação segura das mídias de armazenamento inservíveis para o BPEB de forma a impedir a recuperação de dados e eventuais vazamentos de informação.

Art. 15. Da utilização dos serviços da rede interna:

I – a criação de contas para o acesso de qualquer militar aos serviços da rede interna será condicionada à publicação em BI da designação para sua respectiva função e deverá observar o princípio do privilégio mínimo;

II – a exclusão das contas de acesso aos diversos sistemas para usuários a serem desligados do BPEB se dará no momento em que for solicitada a assinatura do "Nada Consta" à Seção de Informática. Só após a exclusão das contas o "Nada Consta" poderá ser assinado pelo Chefe da Seção de Informática.

III – uma vez cadastrado, o militar é o responsável por manter os privilégios de acesso aos diversos sistemas, devendo este solicitar a Seção de Informática a atualização de seu privilégio de acesso quando necessário ou quando houver mudança de função;

IV – o serviço de e-mail corporativo destina-se a assuntos profissionais, não devendo seus usuários utilizá-lo para cadastro em sítios que não tenham relação com suas atividades profissionais;

V – é proibida aos usuários do serviço de e-mail disponível na rede interna a utilização deste para a disseminação de propagandas, de conteúdo que atente contra a ética e pundonor militar, bem como de qualquer matéria que não esteja relacionada a atividades profissionais;

VI – é proibida a tramitação via e-mail corporativo de qualquer documento que tenha classificação sigilosa com grau igual ou mais restrito a RESERVADO;

VII – é proibido o acesso através da rede interna desta OM a qualquer sítio que disponibilize matéria considerada ilícita, contrária à disciplina militar, à moral e aos bons costumes, bem como atentatória à ordem pública ou que viole qualquer direito de terceiros;

VIII – o acesso a redes sociais via rede interna do BPEB poderá ser realizado de forma controlada e desde que não interfira no desempenho da rede interna ou no bom andamento do serviço;

IX – é proibido o armazenamento no servidor de arquivos desta OM matéria considerada ilícita, contrária à disciplina militar, à moral e aos bons costumes, bem como atentatória à ordem pública, ou que viole qualquer direito de terceiros;

X – é proibido aos usuários da rede interna armazenar de forma permanente documentos relativos à sua atividade profissional em sua estação de trabalho. Para este armazenamento deverá ser utilizado o servidor de arquivos da rede interna;

XI – as telas de bloqueio e os planos de fundo das estações de trabalho desta OM serão os padronizados para a distribuição GNU/Linux do BPEB.

Art. 16. Da política de cópia de segurança:

I – a cópia de segurança dos sistemas utilizados na rede interna do BPEB (servidor de arquivos, SPED, etc), deverá ser executada pela Seção de Informática;

II – a Seção de Informática deverá elaborar, apresentar e executar um plano de backup dos sistemas utilizados na rede interna do Centro (servidor de arquivos, SPED, etc);

III – a Seção de Informática será responsável apenas pela cópia de segurança dos arquivos que estiverem nos sistemas utilizados na rede interna desta OM. Arquivos em estações de trabalho serão de responsabilidade de seus usuários;

IV – a Seção de Informática deverá executar o processo de validação das cópias de segurança pelo menos uma vez por semana.

V – os processos de execução e validação de backups realizados pela Seção de Informática serão auditados por equipes do 7º CTA em suas visitas anuais de orientação técnica.

Art. 17. Da utilização de rede sem fio:

I – a utilização de redes sem fio deverá ser restrita aos laboratórios e para áreas destinadas a visitantes, ficando a utilização em outros ambientes condicionada à necessidade e mediante análise de risco realizada pela Seção de Informática;

II – os dispositivos utilizados para prover o acesso à internet por meio de redes sem fio devem ser configurados de modo a utilizar criptografia, no mínimo padrão Wi-Fi Protected Access II (WPA2) e seus acessos controlados por filtros de endereço Media Access Control (MAC);

III – a Seção de Informática deverá implementar o sistema de controle de acesso aos dispositivos de acesso à rede sem fio, devendo este ser feito com base no endereço Media Access Control (MAC), após cadastro prévio, de forma a individualizar o acesso à Rede Mundial de Computadores;

Art. 18. Da segurança do material de uso geral:

I – toda retirada de material desta OM deverá ser autorizada e documentada;

II – todas as repartições desta OM deverão ser fechadas ao final do expediente, devendo o chefe da Seção zelar pela execução desta norma;

III – é proibida a posse de chaves de qualquer repartição a militar que não seja o chefe ou o responsável pela repartição;

IV – as chaves das repartições guardadas no claviculário deverão ser lacradas e utilizadas apenas mediante autorização do Subcomandante desta OM;

V – o controle do material deverá ser gerenciado e fiscalizado pelos chefes de seção, sendo esses os responsáveis pela efetividade dessas medidas de segurança.

Art. 19. Do controle de acesso físico:

I – o controle de acesso físico deverá obedecer ao previsto no Plano de Desenvolvimento da Contra-inteligência e Plano Diretor de Tecnologia da Informação (PDTI) deste aquartelamento;

II – áreas específicas, como o data center e outras relacionadas à operação terão seu controle de acesso físico regulado em normas próprias de utilização dessas áreas.

Art. 20. Da utilização dos meios telefônicos:

I – os meios telefônicos desta OM deverão ser utilizados apenas para assuntos de natureza ostensiva, ficando vedada a utilização dos meios telefônicos para assuntos de natureza sensível;

II – é proibido o fornecimento de informações pessoais ou de natureza pessoal de qualquer militar do BPEB por telefone.

Art. 21. Das videoconferências:

I – apenas o Comando desta OM ou militar por este designado poderá realizar videoconferências no âmbito corporativo;

II – videoconferências deverão ser realizadas utilizando apenas equipamentos homologados ou autorizados pelo escalão superior;

III – videoconferências realizadas a partir da rede interna desta OM deverão tratar apenas de assuntos de natureza ostensiva.

Art. 22. Do pessoal terceirizado:

I – todo prestador de serviço terceirizado, cujo período de prestação do serviço for superior a 15 (quinze) dias, deverá assinar o Termo de Compromisso e Manutenção de Sigilo, conforme Anexo B;

II – a seção que intermediar a contratação do serviço terceirizado, deverá informar em até três dias úteis antes do início da prestação do serviço os dados necessários à 2ª Seção para a confecção do Termo de Compromisso e Manutenção de Sigilo (nome completo, identidade, CPF, período da prestação do serviço e serviço a ser prestado);

III – a 2ª Seção deverá providenciar para que a assinatura do Termo de Compromisso e Manutenção de Sigilo seja realizada na primeira hora antes do início da prestação do serviço;

IV – a 2ª Seção, por intermédio da Fiscalização Administrativa, deverá providenciar a assinatura do Termo de Compromisso e Manutenção de Sigilo por pessoal terceirizado que já prestar serviço para o Centro;

V – os militares do efetivo variável deverão assinar o Termo de Compromisso e Manutenção de Sigilo por ocasião de sua apresentação nesta OM, ficando a Sargenteação responsável por providenciar esta assinatura, inclusive dos militares do efetivo variável que já integrem o efetivo desta OM;

VI – os militares Prestadores de Tarefa por Tempo Certo (PTTC) deverão assinar o Termo de Compromisso e Manutenção de Sigilo e serão, para fins desta POSIC, considerados como do efetivo deste Centro, tendo assim todos os direitos e responsabilidades destes, inclusive no que tange às penalidades;

VII – a 2ª Seção deverá providenciar a assinatura do Termo de Compromisso e Manutenção de Sigilo para os militares PTTC, conforme modelo do Anexo B;

VIII – caso esta OM venha a ter em seu efetivo alunos/estagiários, estes deverão conhecer e cumprir estas normas, bem como assinar o Termo de Compromisso e Manutenção de Sigilo, estando sujeitos, em caso de infração, às penalidades previstas nesta POSIC;

IX – a 2ª Seção deverá providenciar a assinatura do Termo de Compromisso e Manutenção de Sigilo para os estagiários, conforme modelo do Anexo B e discriminando a Instituição à qual o funcionário é vinculado.

Art. 23. Das penalidades:

I – a violação a estas normas será tratada como descumprimento de ordem, quando não constituir transgressão mais grave, devendo essa ser apurada conforme o Regulamento Disciplinar do Exército (RDE);

II – violações a esta política que configurarem crime serão tratadas à luz da legislação em vigor, seja o Código Penal Militar (CPM), Código Penal ou legislação própria da Administração Pública Federal (APF).

III – a violação destas normas por prestadores de serviço terceirizados ou por estagiários estará sujeita a penalidades de advertência e até rescisão contratual em caso de reincidência;

IV – caso configure crime tipificado no Código Penal Militar (CPM), Código Penal ou legislação própria da Administração Pública Federal (APF), as violações serão apuradas e tratadas na forma da lei.

6. Responsabilidades

Art. 24. Do Comitê Interno de Segurança da Informação e Comunicações (CISIC):

I – o Comitê Interno de Segurança Informação e Comunicações (CISIC) será composto pelo Subcomandante desta OM, seu presidente, e 01 (um) oficial de cada seção diretamente subordinada à chefia, excluindo-se a Seção Informática, que é responsável por realizar auditorias internas de segurança da informação no BPEB;

II – ao CISIC compete:

a) cumprir e fazer cumprir estas normas;

b) divulgar, de forma efetiva, a Política de Segurança da Informação e Comunicações desta OM;

c) promover no âmbito desta OM, através de campanhas, instruções ou por qualquer outro meio conveniente, a cultura de segurança da informação, para isso o CISIC poderá utilizar recursos materiais e humanos disponíveis em qualquer repartição desta OM;

d) fiscalizar o exato cumprimento desta Política;

e) apurar e levar à autoridade competente, para aplicação de penalidades, os casos de infração a estas normas;

f) preparar o BPEB para as auditorias em segurança da informação previstas no Sistema de Telemática do Exército (SisTEx).

Art. 25. Ao presidente do CISIC compete:

I – cumprir e fazer cumprir estas normas;

II – designar os membros do CISIC fazendo constar anualmente no boletim interno da OM a composição do CISIC;

III – dividir entre os membros do CISIC as tarefas e responsabilidades para o fiel cumprimento desta Política;

IV – sendo o presidente do CISIC o Subcomandante desta OM este deverá, quando for o caso, distribuir o Formulário de Apuração de Transgressão Disciplinar (FATD) para apurar infração a estas normas.

7. Do Serviço de Manutenção

Art. 26. A manutenção dos dispositivos computacionais obedecerá aos seguintes critérios:

I – Quando determinado dispositivo computacional deixar de funcionar corretamente, o seu usuário direto deverá acionar a Seção de Informática, que avaliará *in loco* (inicialmente pelo militar da SU) e verificará se a manutenção deve ser feita acionando a garantia do produto, ou na seção de informática, ou ainda manutenção externa:

a) manutenção acionando a garantia:

O material será entregue ao Almoxarifado para fins de envio para manutenção;

b) manutenção na Seção de Informática:

Materiais que puderem ser manutenidos (preditivamente, preventivamente ou corretivamente) pelos militares da Seção de Informática, serão manutenidos, observadas as capacidades técnicas e disponibilidades de material para realização da manutenção no prazo de tempo necessário para solução do problema;

c) manutenção externa:

Materiais que não puderem ser manutenidos pelos militares da Seção de Informática e que não estiverem na garantia serão encaminhados dentro da viabilidade (custo de manutenção não poderá ultrapassar de 50% do seu valor), possibilidade e disponibilidade (pregões e atas de serviços existentes) para fins de manutenção.

8. Prescrições Diversas

Art. 27. Das prescrições diversas:

I – esta política entra em vigor na data de sua publicação;

II – este documento deverá ser disponibilizado na intranet desta OM;

III – a Seção de Informática deverá, como parte dos trabalhos de conscientização e em coordenação com o S2, preparar e apresentar instrução para todos os integrantes do BPEB a fim de que todos os membros deste aquartelamento tenham inteira compreensão da finalidade e objetivos desta política, bem como o conhecimento de seus direitos e deveres no tocante à execução desta;

IV – implementações que por ventura forem necessárias deverão ser providenciadas pelo Comitê Interno de Segurança da Informação e Comunicações (CISIC);

V – implementações que por sua complexidade necessitarem de recursos financeiros, deverão ser planejadas e executadas em consonância com as Normas vigentes na Administração Pública Federal;

VI – a 2ª Seção será responsável pela posse e arquivamento dos Termos de Compromisso e Manutenção de Sigilo assinados em acordo com esta política;

VII – ações que violarem qualquer um dos pilares da segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade) e que por ventura não constem neste documento não eximem seu executor de responsabilidade e serão apuradas à luz do Regulamento Disciplinar do Exército (RDE), se não constituir crime capitulado no Código Penal Militar (CPM), Código Penal ou em legislação própria da Administração Pública Federal.

(Solução ao DIEx Nr 544 - Sec Inf/Cia C Sv/BPEB, de 30 MAIO 17).

Em consequência, S/1, Cmt SU e demais interessados tomem as providências decorrentes.

4ª Parte

JUSTIÇA E DISCIPLINA

1. **JUSTIÇA**

Sem alteração.

2. **DISCIPLINA**

Sem alteração.

MAURÍCIO DE SOUZA BEZERRA – Cel
Comandante do Batalhão de Polícia do Exército de Brasília