POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

4º BATALHÃO DE INFANTARIA LEVE

# 1. FINALIDADE

Art. 10 Este documento tem por finalidade estabelecer Diretrizes de Segurança da Informação e Comunicações a serem adotadas pelos integrantes do 4º Batalhão de Infantaria Leve (4º BIL), 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. 20 Constituem propósitos destas Diretrizes:

1. — formalizar direitos e responsabilidades de usuários e administradores de redes e sistemas

do 4º BIL;

1. — garantir o bom uso dos recursos de Tecnologia da Informação e Comunicações (TIC) do

4º BIL;

1. — atribuir papeis e responsabilidades na elevação dos níveis de segurança da informação

no âmbito do 4º BIL;

1. — disseminar a cultura de segurança da informação no âmbito do 4º BIL.

2. OBJETIVOS

Art. 30 São objetivos desta Política:

1 - definir e estabelecer procedimentos relacionados à Segurança da Informação e

Comunicações a serem adotados pelos integrantes do 4º BIL;

1. — normatizar, no âmbito do 4º BIL, o uso dos recursos de TIC;
2. — estabelecer regras para o controle de acesso aos recursos de TIC e à Rede Mundial de Computadores a partir da rede local desta OM;
3. — atribuir papeis e responsabilidades na utilização, operação e manuseio dos recursos computacionais do 4º BIL.

# 3. CONCEITOS E PRESSUPOSTOS BÁSICOS

Art. 40 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. 50 Entende-se por dispositivo móvel qualquer tipo de notebook, tablet, smartphone, telefone celular ou equipamentos similares a estes.

Art. 60 Os dispositivos de TI incluídos no patrimônio do 4º BIL são colocados à disposição dos seus militares para uso exclusivo em atividades estritamente relacionadas às funções institucionais por eles desempenhadas.

Art. 70 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. 80 A fim de facilitar a compreensão deste documento e elucidar conceitos, as seguintes definições são necessárias:

1. — ameaças: condições que podem causar incidentes por meio da descoberta de vulnerabilidades;
2. — antivírus: programa que detecta e anula ou remove malwares de um computador;
3. — ativo: a informação em si ou qualquer 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;
4. — backup: cópia de segurança ou meio de armazenamento secundário que contém uma reprodução da informação de arquivos ou conjunto de dados;
5. — correio eletrônico (e-mail): ferramenta que possibilita a transferência de mensagens e qualquer outro documento eletrônico para fins de comunicação;
6. — 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;
7. — 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);
8. — estação de trabalho: computador com recursos voltados para a produtividade pessoal e que completa suas necessidades com recursos de outros computadores na rede;
9. — 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;
10. — 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;
11. — 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;
12. — informação: principal ativo das corporações e que requer grande proteção, de acordo com o seu valor para a organização;
13. — informação sensível: toda e qualquer informação que quando utilizada de maneira inadequada pode causar prejuízos financeiros, material ou à imagem de pessoas ou instituições. Exemplo 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;
14. — log: registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer 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;
15. — NTP (Network Time Protocol): protocolo para sincronização dos relógios dos sistemas e computadores;
16. — risco: probabilidade de exploração das vulnerabilidades pelas ameaças, causando impacto na organização;
17. — software: componente lógico e intangível de um computador, que engloba arquivos executáveis, bibliotecas, programas e sistemas operacionais;
18. — usuários internos: militares integrantes do 4º BIL ou civis autorizados que se encontrem prestando serviço para esta OM ;
19. — usuários externos: todos os usuários de organizações externas que, direta ou indiretamente, acessam os recursos de TIC disponibilizados pelo 4º BIL, incluindo-se os empregados de empresas prestadoras de serviços terceirizados e consultores autorizados a utilizar em caráter temporário os recursos tecnológicos desta OM;
20. — 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;
21. — e-mail corporativo pessoal: serviço de correio eletrônico provido pela instituição ao militar que está cadastrado no Banco de Dados do Exército Brasileiro (EB Corp), este serviço é disponibilizado no sítio ebcloud e fica ativo pelo tempo que o militar permanecer na instituição (exemplo: nomedeguerra.primeironome@eb.mil.br);
22. — e-mail corporativo funcional: serviço de correio eletrônico gerenciado pelas Seções de Informática das OM do Exército Brasileiro podendo ser disponibilizado ou não pelo CT/CTA da Área, tem como finalidade disponibilizar um contato institucional das diversas seções e (ou) divisões da OM permitindo que o militar que utiliza tal serviço transmita, ao se desligar da OM/Seção/Divisão, os e-mails e os contatos que eram recebidos por ele para o novo integrante da OM/Seção/Divisão (exemplo: seção/divisão@om.eb.mil.br).

# 4. REFERÊNCIAS

Art. 90 São referências para este documento:

1. — Constituição da República Federativa do Brasil — 1988;
2. — Lei no 9.296, de 24 de julho de 1996 — Regulamenta o inciso XII, parte final, do Art 5 0 da Constituição Federal, sobre a interceptação de comunicações telefônicas;
3. — Lei 12.737, de 30 de novembro de 2012;
4. — Norma Complementar no 03/1N01/DSIC/GSIPR — Diretrizes para a Elaboração de

Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

1. — Decreto-Lei NO 1.001, de 21 de outubro de 1969 — Código Penal Militar;
2. — Decreto no 4.346, de 26 de agosto de 2002 — Regulamento Disciplinar do Exército (R-
3. — Decreto No 7.845, de 14 de novembro de 2012;
4. — Portaria NO 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 NO 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 NO 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 1309);

1. — Portaria NO 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);
2. — Portaria NO 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);
3. — Portaria NO 011-DCT, de 29 de março de 2010 — Aprova o Plano de Migração para Software Livre no Exército Brasileiro, versão 2010;
4. — Portaria NO 720-Cmt Ex, de 21 de novembro de 2011 — Aprova a Cartilha

Emergencial de Segurança da Tecnologia da Informação e Comunicações (Versão 1.0);

1. - of No 573 -A2.C/DCT - CIRCULAR, de 13 de novembro de 2009;
2. - DIEx no 2-SEC INTLG/DCT, de 21 de janeiro de 2014;
3. Portaria No 1.067, de 8 de setembro de 2014 — Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EBIO-IG-OI.OII), 1a Edição, 2014.

# 5. REGRAS DE SEGURANÇA

Art. 10 São regras gerais:

1. — todos os integrantes do 4º BIL são responsáveis pela elevação dos níveis de segurança da informação no âmbito desta OM;
2. — todo militar usuário dos recursos de TIC deverá assinar o Termo de Compromisso e Manutenção de Sigilo, conforme modelo do Anexo A;
3. — todo militar usuário dos recursos de TIC deverá ter o exato conhecimento destas regras;
4. — será adotado no âmbito do 4º BIL, 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;
5. — a impressão de documento, nas impressoras disponibilizadas pelo 4º BIL, 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 desta OM;
6. — todo documento inservível que contenha informações sensíveis deverá ser picotado e descartado em lixeira adequada;
7. — será adotado no 4º BIL a política de mesa e tela limpa, ou seja, os usuários dos recursos de TIC 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;
8. — toda informação produzida, manuseada ou arquivada deverá passar por uma avaliação crítica quanto à classificação sigilosa;
9. — o protocolo, o envio e o arquivamento de documentos com classificação sigilosa será realizado pela Seção de Inteligência;
10. — todos os documentos sigilosos deverão ser protocolados, mesmo os de natureza interna;
11. — 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;
12. — caso seja necessária a utilização de serviço de armazenamento em nuvem, poderá ser utilizada a solução disponibilizada pelo Cloud - 4º BIL. Contudo, apenas documentos de natureza ostensiva poderão ser armazenados em tal serviço;
13. — 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 nesta OM;
14. — 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 de todas as estações de trabalho e servidores utilizados pelos usuários internos.

Art. 11 Do acesso às redes externas EBNEt e Internet:

1. — o credenciamento para acesso aos sistemas utilizados será feito mediante cadastro de usuário e senha, conhecimento desta Política e assinatura do Termo de Compromisso e Manutenção de Sigilo;
2. — 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;
3. — é proibido o compartilhamento de usuário e senha para acesso a qualquer sistema.
4. — é proibido o acesso, através da rede interna, 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;
5. — o acesso a redes sociais via rede interna poderá ser realizado de forma controlada e desde que não interfira no desempenho da própria rede ou das atividades das profissionais.

Art. 12 Do acesso e uso dos Sistemas Corporativos:

1. — o Sistema de Protocolo Eletrônico de Documentos (SPED) somente deverá ser utilizado para a produção de documentos de caráter ostensivo;
2. — Todo acesso aos Sistemas Corporativos será feito mediante autenticação de senha pessoal e intransferível;
3. — O uso dos Sistemas Corporativos será franqueado para oficiais e sargentos da ativa, Designados para o Serviço Ativo (DSA) e Prestadores de Tarefa por Tempo Certo (PTTC);
4. - O uso dos Sistemas Corporativos por Cabos e Soldados NB e EV serás restrito e deverá ser solicitado por seu chefe de Seção para Seção de Informática 4º BIL.

Art. 13 Do acesso e uso das contas VPN (Virtual Private Network):

1. — a necessidade de abertura e fechamento de contas VPN deverão ser solicitadas à Seção de Informática 4º BIL;
2. — As contas abertas para os militares do 4º BIL serão gerenciadas pelo 30 CTA;
3. — As contas VPN tem a validade de um ano após a data de sua criação. As renovações deverão ser solicitadas à Seção de Informática 4º BIL;
4. — Após o primeiro acesso o usuário da conta deverá alterar a senha inicial pelo site **senha.vpn.cmsecloud.eb.mil.br/UCP**;
5. — A política de senha das conas VPN é coordenada pelo 30CTA e tem as seguintes premissas: mínimo de 08 caracteres; diferente do nome do usuário ou sua ordem reversa; não repetição de caracteres 4 ou mais vezes consecutivamente; conter obrigatoriamente 01 caractere alfabético maiúsculo, 01 caractere alfabético minúsculo, 01 caractere numérico e 01 caractere especial.

Art. 14 Do acesso e uso do correio eletrônico corporativo:

1. — O serviço de correio eletrônico pessoal corporativo é prestado pelo CDS/CITEx e será gerenciado pelo próprio usuário no site https://ebcloud.eb.mil.br/;
2. — O serviço de correio eletrônico funcional corporativo é disponibilizado pelo 30CTA e gerenciado pela Seção de Informática 4º BIL;
3. — é proibido 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;
4. — o serviço de e-mail corporativo destina-se a assuntos profissionais, não devendo seu usuários utilizá-lo para cadastro em sítios que não tenham relação com suas atividades profissionais;
5. — é proibida a tramitação via e-mail corporativo de qualquer documento que tem a classificação sigilosa com grau igual ou mais restrito a RESERVADO;
6. — poderá ser utilizado o serviço de correio eletrônico corporativo para troca e 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.

Art. 15 Do acesso à Rede Interna de Armazenamento de dados:

1. — 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;
2. — a exclusão das contas de acesso aos diversos sistemas para usuários a serem desligados do 4º BIL se dará no momento em que for solicitada a assinatura do "Nada Consta" à Seção de Informática do 4º BIL. Só após a exclusão das contas o "Nada Consta" poderá ser assinado pelo Seção de Informática do 4º BIL.
3. — 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;
4. — é proibido o armazenamento no servidor de arquivos 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;
5. — 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;
6. — as telas de bloqueio e os planos de fundo das estações de trabalho desta OM devem ser padronizados para todos os usuários de TIC.
7. – **o uso de notebook e computadores particular na rede interna do 4º BIL, só será permitido somente com autorização por escrito do Cmt 4º BIL, para isso tendo uma justificativa plausível para o uso do mesmo.**

Art. 16 Das cópias de Segurança (Backup):

1. — a cópia de segurança dos sistemas utilizados na rede interna do 4º BIL (servidor de arquivos, SPED, servidor de e-mail, etc), deverá ser executada pela Seção de Informática do 4º BIL;
2. — a Seção de Informática do 4º BIL deverá elaborar, apresentar e executar um plano de backup dos sistemas utilizados na rede interna;
3. — a Seção de Informática do 4º BIL 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 salvarem os mesmos no Servidor de Arquivo;**
4. — a Seção de Informática do 4º BIL deverá executar o processo de validação das cópias de segurança pelo menos uma vez por semana.

Art. 17 Da segurança do software:

I - **fica padronizado para utilização no âmbito da rede interna, o sistema operacional GNU/Linux, ficando as exceções restritas aos casos absolutamente necessários e sob a avaliação da Seção de Informática do 4º BIL;**

II — sistemas operacionais que necessitam de antivírus devem utilizar a solução institucional configurada para ser atualizada automaticamente. Na ausência de uma solução institucional, dever ser utilizado o software livre conforme orientação do CITEx;

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

1. — apenas a Seção de Informática do 4º BIL, por meio de solicitação via sistema de gerenciamento de parque computacional, tem autorização para instalar, remover ou modificar sistemas operacionais instalados na rede interna;
2. — apenas a Seção de Informática do 4º BIL deverá possuir senha de administrador (root) nos sistemas operacionais da rede interna e providenciar para que os usuários tenham acesso apenas como usuários comuns;
3. — 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;
4. — deverá ser executado o hardening básico dos sistemas operacionais para os usuários internos, atentando para que estes não percam funcionalidades básicas.
5. — a Seção de Informática do 4º BIL deverá implementar mecanismo de descarte ou de alienação segura das mídias de armazenamento inservíveis de forma a impedir a recuperação de dados e eventuais vazamentos de informação.

Art. 18 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;

1. — deverá haver trimestralmente a conferência do material existente nas seções desta OM, devendo as alterações serem informadas de forma documentada à Divisão Administrativa;
2. — o material de TI destinado a consumo deverá ser controlado, ficando a cargo da Seção de Informática do 4º BIL a execução desse controle;
3. — todo material de TI retirado do aquartelamento, sob cautela, deverá estar autorizado pelo Chefe da Divisão Administrativa e pelo Chefe da Divisão ou Seção à qual o material pertença;
4. — microcomputadores pertencentes ao parque computacional do 4º BIL deverão estar lacrados e com seus componentes e acessórios controlados por meio de sistema automatizado de inventário;
5. — ativos de rede deverão ser acondicionados em armários chaveados, de forma a impedir o livre acesso aos mesmos;
6. — é proibida a mudança da disposição dos ativos de TI sem a devida autorização da Seção de Informática do 4º BIL e dos chefes de divisão ou seção envolvidos, e sem a realização prévia de uma análise de risco;
7. — a Seção de Informática do 4º BIL deverá controlar o processo de lacre e cadastramento no sistema de inventário dos microcomputadores do parque computacional. Apenas a Seção de Informática do 4º BIL, mediante abertura de chamado em sistema de gerenciamento de parque computacional, está autorizada a romper lacre e substituir acessórios ou componentes dos microcomputadores.
8. — é expressamente proibida a utilização de dispositivos móveis pessoais na rede de dados do 4º BIL;

X — o compartilhamento de arquivos deverá ocorrer utilizando-se os serviços fornecidos pelo 4º BIL (servidor de arquivos, servidor de e-mail ou quando for o caso servidor FTP), sendo proibida a utilização de pen drives e HDs externos pessoais ou quaisquer dispositivos similares a estes; — poderá ser utilizado, para trâmite de arquivos entre esta OM e órgãos externos, apenas dispositivos móveis institucionais. Esse uso, contudo, deve ser evitado e caso seja necessário, o dispositivo deverá ser criptografado;

1. — notebooks institucionais deverão ter seus discos rígidos criptografados;
2. — notebooks institucionais deverão ser configurados para não armazenarem cookies e históricos em seus navegadores;
3. — 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 do 4º BIL para a administração do sistema operacional.

Art. 19 Da utilização de rede sem fio:

1. — a utilização de redes sem fio deverá ser restrita a laboratórios, ficando a utilização em outros ambientes condicionadas à necessidade e mediante análise de risco realizada pela Seção de Informática do 4º BIL,
2. — 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);
3. — a Seção de Informática do 4º BIL 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.

Art. 20 Do controle de acesso físico:

1. — o controle de acesso físico deverá obedecer ao previsto no Plano de Segurança Orgânica deste aquartelamento;
2. — áreas específicas, como sala de servidores ou centros de operações, terão seu controle de acesso físico regulado em normas próprias.

Art. 21 Da utilização dos meios telefônicos:

1. — os meios telefônicos deverão ser utilizados apenas para assuntos de natureza ostensiva, ficando vedada a utilização dos meios telefônicos para assuntos de natureza sensível;
2. — é proibido o fornecimento de informações pessoais ou de natureza pessoal de qualquer militar do 4º BIL por telefone.

Art. 22 Das videoconferências:

1. — videoconferências deverão ser realizadas utilizando apenas equipamentos homologados ou autorizados pelo escalão superior;
2. — videoconferências realizadas a partir da rede interna deverão tratar apenas de assuntos de natureza ostensiva.

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 do 4º BIL, seu presidente, e 01 (um) oficial de cada Seção diretamente subordinada;

11 - ao CISIC compete:

1. cumprir e fazer cumprir estas normas;
2. divulgar, de forma efetiva, a Política de Segurança da Informação e Comunicações desta OM;
3. promover 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;
4. fiscalizar o exato cumprimento desta Política;
5. apurar e levar à autoridade competente, para aplicação de penalidades, os casos de infração a estas normas;
6. preparar o 4º BIL para as auditorias em segurança da informação previstas no Sistema de Telemática do Exército (SisTEx), Centro de Inteligência do Exército e Inspetoria de Contabilidade e Finanças.

Art. 25 Ao presidente do CISIC compete:

1. — cumprir e fazer cumprir estas normas;
2. — designar os membros do CISIC fazendo constar anualmente no boletim interno 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 do 4º BIL, este deverá, quando for o caso, distribuir o Formulário de Apuração de Transgressão Disciplinar (FATD) para apurar infração a estas normas.

Art. 26 Das penalidades:

1. — 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);
2. — 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).
3. — 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;
4. — 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.
5. — 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.

# 7. PRESCRIÇÕES DIVERSAS

Art. 27 Das prescrições diversas:

1. — esta Política entra em vigor na data de sua publicação;
2. — este documento deverá ser disponibilizado na intranet desta OM;
3. — a Seção de Informática do 4º BIL deverá, como parte dos trabalhos de conscientização, preparar e apresentar instrução para todos os integrantes do 4º BIL a fim de que todos os membros tenham inteira compreensão da finalidade e objetivos desta política, bem como o conhecimento de seus direitos e deveres no tocante à execução desta;
4. — implementações que por ventura forem necessárias deverão ser providenciadas pela Seção de Informática do 4º BIL;
5. — implementações que por sua complexidade necessitarem de recursos financeiros, deverão ser planejadas e executadas em consonância com as Normas vigentes na Administração Pública Federal;
6. — a 2ª Seção do 4º BIL será responsável pela posse e arquivamento dos Termos de Compromisso e Manutenção de Sigilo assinados em acordo com esta política.

**LEANDRO ATAIDO ACOSTA – CEL**

**CMT 4º BIL**