POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC/IMBEL)

ORIGEM

Coordenadoria-Geral de Tecnologia da Informação e Comunicações - CGTIC

REFERÊNCIAS LEGAIS E NORMATIVAS

Decreto nº 9.573, de 22 de novembro de 2018;
Decreto nº 9.637, de 26 de dezembro de 2018;
Decreto nº 7.579, de 11 de outubro de 2011;
Decreto nº 8.638, de 15 de janeiro de 2016;
Decreto nº 7.845, de 14 de novembro de 2012;
e-PING / 2018;
NBR ISO 31000:2009;
NBR ISO/IEC 27005:2011;
NBR ISO/IEC 27001:2013;
NBR ISO/IEC 27002:2013;
NC03/IN01/GSI/PR/GSI, de 30 de junho de 2009;
NC20/IN01/DSIC/GSIPR, de 15 de dezembro de 2014;
NC14/IN01/DSIC/GSIPR - Portaria nº 9, de 15 de março de 2018;
IN01/GSI, de 13 de junho de 2008;
IN 01, de 04 de abril de 2019; e
O.T.31.N.001 – STI – Norma Corporativa, Rev. 00, de 01/09/2010, da IMBEL.

CAMPO DE APLICAÇÃO

Esta Política se aplica no âmbito da Indústria de Material Bélico do Brasil – IMBEL

APROVAÇÃO

Aprovado na 325ª reunião do Conselho de Administração da IMBEL.
(Resolução nº 41/2019 – CA/IMBEL, 18 de dezembro de 2019)

Brasília – DF
Dezembro 2019

SUMÁRIO

O PRESIDENTE DA IMBEL, no uso da atribuição que lhe confere o art. 16, em seu inciso VI, do Regimento Interno da IMBEL.

Publica:

1. OBJETIVO

1.1. Estabelecer diretrizes, critérios e procedimentos a serem adotados pelos funcionários da IMBEL, no tocante à Segurança da Informação e Comunicações.
1.2. São objetivos da Política de Segurança da Informação e Comunicações (POSIC):
1.2.1. A instituição de diretrizes estratégicas, responsabilidades e competências que visam garantir a disponibilidade, integridade, confidencialidade, autenticidade das informações e responsabilidades, visando assegurar os serviços da empresa, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso da Indústria de Material Bélico do Brasil (IMBEL) contra ameaças e vulnerabilidades.
1.2.2. Preservar os seus ativos de informação, assim como a sua imagem institucional.
1.2.3. Orientar a IMBEL no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e Comunicações (SIC), em conformidade com as disposições constitucionais, legais e regimentais vigentes.
1.2.4. Estabelecer o comprometimento da Alta Direção Organizacional da Empresa, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança da Informação e Comunicações (GRSIC);
1.2.5. Contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais;
1.2.6. Aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação;
1.2.7. Fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação; e
1.2.8. Fortalecer a cultura da segurança da informação.

2. CONSIDERAÇÕES INICIAIS

2.1. Para os efeitos desta Política entende-se como “Sistema IMBEL”, as seguintes unidades: A IMBEL Sede, localizada em Brasília-DF, a Fábrica Estrela (FE), localizada na cidade de Magé-RJ, a Fábrica de Itajubá (FI), localizada em Itajubá-MG, a Fábrica Presidente Vargas (FPV), localizada em Piquete - SP, a Fábrica de Juiz de Fora (FJF), localizada na cidade de Juiz de Fora - MG, a Fábrica de Material de Comunicações e Eletrônica (FMCE), situada na cidade do Rio de Janeiro-RJ e a Rede Elétrica Piquete-Itajubá (REPI), localizada na cidade de Wenceslau Braz-MG;
2.2. A Política de Segurança da Informação e Comunicações (POSIC) aplica-se a todas as Unidades Administrativas (UA), funcionários e colaboradores externos que prestam serviço em razão de contratos administrativos firmados na forma da Lei e, no

que couber, no relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação de qualquer tipo, convênios e termos congêneres;

2.3. A Política de Segurança da Informação e Comunicações (POSIC) tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue;

2.4. Fica instituída a Política de Segurança da Informação e Comunicações (POSIC), no âmbito da Indústria de Material Bélico do Brasil (IMBEL), com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e autenticidade da informação na Empresa; e

2.5. As diretrizes constantes nesta Política de Segurança, no âmbito do órgão ou entidade, visam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

3. CONCEITOS E DEFINIÇÕES

3.1. Para os efeitos desta Política são estabelecidos os seguintes conceitos e definições:

3.1.1. **Ativo –** É tudo o que pode ter ou fornecer um valor para uma organização. A definição de um **ativo** na norma ABNT NBR ISO/IEC 27002 - Código de Prática para a Gestão de Segurança da **Informação** é bem sucinta: **Ativo**: qualquer coisa que tenha valor para a organização. No âmbito desta POSIC, são considerados ativos da IMBEL: a informação em si em qualquer meio de comunicação, softwares, ativos físicos, serviços, as pessoas e suas qualificações e os ativos intangíveis, tais como reputação e imagem da Empresa;

3.1.2. **Estrutura de SIC -** é o conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

3.1.3. **Defesa Cibernética -** o "conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente." (EME, Brasília, 2010);

3.1.4. **Segurança Cibernética -** é um conjunto de ações sobre pessoas, tecnologias e processos contra os ataques cibernéticos. A Segurança Cibernética, assim como a Digital, é uma ramificação dentro da Segurança da Informação;

3.1.5. **Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT.br) -** é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo **NIC.br**, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de

segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CERTs no Brasil. Estas atividades têm como objetivo estratégico aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil;

3.1.6. **Comitê Gestor de Segurança da Informação e Comunicações (CGSIC) –** grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da IMBEL;

3.1.7. **Dado -** é um conjunto de valores ou ocorrências em um estado bruto com o qual são obtidas informações com o objetivo de adquirir benefícios. Existem dois tipos de dados: estruturados e não estruturados. Os dados estruturados, que são dados formatados, organizados em tabelas - linhas e colunas - e são facilmente processados, geralmente é utilizado um sistema gerenciador de banco de dados para armazenar esse tipo de dado, um exemplo são os dados gerados por aplicações empresariais. Os dados não estruturados não possuem uma formatação específica e são mais difíceis de serem processados. Por exemplo, mensagens de e-mail, imagens, documentos de texto e mensagens em redes sociais;

3.1.8. **Gestão de Continuidade do Negócio (GCN) –** é uma abordagem integrada que envolve a mobilização de toda a organização para gerenciar crises e recuperar as operações após a ocorrência de qualquer evento que cause uma ruptura operacional;

3.1.9. **Gestor de Segurança da Informação e Comunicações (GSIC) –** é responsável pelas ações de segurança da informação e comunicações no âmbito da IMBEL;

3.1.10. **Indústria de Material Bélico do Brasil (IMBEL) –** É uma empresa Estratégica de Defesa, constituída nos termos da Lei nº 6.227, de 14 de julho de 1975. É uma empresa pública dependente, com personalidade jurídica de direito privado, vinculada ao Ministério da Defesa por intermédio do Comando do Exército, com a missão de fabricar e comercializar produtos de defesa e segurança para clientes institucionais, especialmente Forças Armadas, Forças Policiais e clientes privados;

3.1.11. **Incidentes de Segurança da Informação -** Segundo CERT.br, um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores. Em geral, toda situação onde uma entidade de informação está sob risco é considerado um incidente de segurança;

3.1.12. **Informação -** A informação é a ordenação e organização dos dados de forma que passa a transmitir uma mensagem compreensiva dentro de um determinado contexto. Um conjunto de dados que transmite conhecimento é uma informação;

3.1.13. **Núcleo de Informação e Coordenação do Ponto BR (NIC.br) -** é uma associação, sem fins lucrativos, criada 08 de março de 2005 pelos membros do Comitê Gestor da Internet no Brasil (CGI.br), para a execução do registro de Nomes de Domínio, alocação de endereços IP e administração do ccTLD.br.

3.1.14. **Plano Setorial -** é uma ferramenta de planejamento, em que estão descritos os projetos e as ações relevantes que o órgão ou unidade administrativa pretende realizar durante um exercício (um ano), contemplando desdobramentos do plano estratégico;

3.1.15. **Política de Segurança da Informação e Comunicações (POSIC) –** documento aprovado pela autoridade responsável pela empresa, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficiente à implementação da segurança da informação e comunicações;

3.1.16. **Quebra de Segurança –** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

3.1.17. **Segurança da informação classificada -** existem informações cuja divulgação indiscriminada pode colocar em risco a segurança da sociedade ou do Estado. Por isso, apesar de públicas, o acesso a elas deve ser restringido por um determinado tempo. A LAI (Lei de Acesso à Informação) prevê que tais informações podem ser classificadas como reservadas, secretas e ultrassecretas, conforme estabelecido no art. 23 da LAI;

3.1.18. **Segurança das infraestruturas críticas -** definidas como o subconjunto de ativos de informação - meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso - que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade;

3.1.19. **Serviços Críticos de TI –** são os serviços que foram monitorados, observados e analisados a fim de perceber alterações que devem ser corrigidas. O monitoramento dos serviços críticos vai além de somente garantir que tudo está funcionando. Busca entender, também, se existem brechas que podem, eventualmente, causar falhas nos sistemas e gerar prejuízos para a empresa. Esse é o estágio inicial para um processo de tomada de decisão mais ágil, que busca otimizar a alocação dos recursos de TI e reduzir os custos com possíveis paradas nos sistemas ou com manutenções; e

3.1.20. **Unidades Administrativas (UA) -** é aquela que possui três características: pessoal, patrimônio e competências próprias. Não é critério necessário ter orçamento para se dizer que uma unidade é administrativa.

3.2. **Os 4 Princípios da Segurança da Informação são:** a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

3.2.1.1. **Autenticidade –** Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação;

3.2.1.2. **Confidencialidade –** garantir que a informação estará acessível apenas para pessoas autorizadas. A principal forma de mantê-la é por meio da autenticação,

controlando e restringindo os acessos. Ela impõe limitações aos milhares de dados sigilosos que as empresas possuem;

3.2.1.3. **Disponibilidade –** Os dados corporativos precisam estar seguros e disponíveis para serem acessados a qualquer momento pelos usuários autorizados. Esse princípio diz respeito à eficácia do sistema e do funcionamento da rede para que seja possível utilizar a informação quando necessário. Ela deve ser hospeda em um sistema à prova de falhas lógicas e redundantes. Na hora de gerar relatórios para auditoria, por exemplo, é necessário que os dados possam ser facilmente encontrados e processados. Esse é o princípio da disponibilidade; e

3.2.1.4. **Integridade –** O princípio de integridade refere-se à manutenção das condições iniciais das informações de acordo com a forma que foram produzidas e armazenadas. Ou seja, a informação mantém sua origem e ela não pode ser alterada, assim somente pessoas autorizadas poderão acessar e modificar os dados do sistema. Quando o processo é executado estrategicamente é possível utilizar ferramentas para realizar a recuperação de informações danificadas ou perdidas.

4. PRINCÍPIOS

4.1. São princípios da POSIC:

4.1.1. Respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

4.1.2. Visão abrangente e sistêmica da segurança da informação;

4.1.3. Responsabilidade da Presidência da IMBEL na coordenação de esforços e no estabelecimento de políticas, estratégias e diretrizes relacionadas à segurança da informação;

4.1.4. Preservação do acervo histórico da IMBEL;

4.1.5. Educação como alicerce fundamental para o fomento da cultura em segurança da informação;

4.1.6. Orientação à gestão de riscos e à gestão da segurança da informação;

4.1.7. Prevenção e tratamento de incidentes de segurança da informação;

4.1.8. Articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação;

4.1.9. Dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas; e

4.1.10. Integração e cooperação entre o Poder Público, o Setor Empresarial, a Sociedade e as Instituições Acadêmicas.

5. DIRETRIZES GERAIS

5.1. **Tratamento da Informação:**

5.1.1. Para assegurar a proteção adequada às informações, deve existir um método de classificação da informação de acordo com o grau de confidencialidade e criticidade para o negócio da IMBEL;

5.1.2. As informações devem ser atribuídas a um proprietário, formalmente designado como responsável pela autorização de acesso às informações sob a sua responsabilidade;

5.1.3. Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da IMBEL em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;

5.1.4. A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;

5.1.5. A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços da IMBEL;

5.1.6. Os dados, as informações e os sistemas de informação da IMBEL devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens; e

5.1.7. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade, elaborando-se, para tanto, sistema de classificação da informação.

5.2. **Tratamento de Incidentes de Rede:**

5.2.1. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, pelas áreas responsáveis pelos respectivos ativos de informação impactados, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos da IMBEL, sem prejuízo de sua comunicação à Estrutura de SIC (Segurança da Informação e Comunicações) da empresa.

5.3. **Gestão de Riscos:**

5.3.1. A Estrutura de Segurança da Informação e Comunicações (SIC) da IMBEL deverá estabelecer metodologia que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e os riscos;

5.3.2. As unidades administrativas da empresa, com apoio da Estrutura de SIC da IMBEL, deverão implementar as atividades de gestão dos riscos de segurança da informação e comunicações associadas aos ativos de informação sob sua responsabilidade;

5.3.3. Os riscos de SIC deverão ser considerados na contratação de serviços terceirizados, sendo os gestores das unidades administrativas e dos ativos relacionados, os gestores e fiscais de contrato, bem como os fornecedores e

custodiantes, os responsáveis por manter os níveis apropriados de segurança da informação na entrega dos serviços; e

5.3.4. As normas e procedimentos da IMBEL devem considerar controles para a troca de informações, tanto interna quanto externamente, de forma a manter o nível adequado de segurança da informação e comunicações.

5.4. **Gestão de Ativos:**

5.4.1. A Estrutura de SIC da IMBEL deve instituir normas e procedimentos que garantam a adequada gestão dos ativos da empresa, em conjunto com as unidades responsáveis pelos respectivos ativos;

5.4.2. A gestão dos ativos deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;

5.4.3. Todos os ativos deverão ser classificados em termos de valor, requisitos legais, sensibilidade e criticidade para a Instituição;

5.4.4. Ações e controles específicos de segurança deverão garantir a proteção adequada dos ativos, em níveis compatíveis ao seu grau de importância para a consecução das atividades e objetivos estratégicos da empresa;

5.4.5. Os ativos devem ser associados a controles de segurança implementados independentemente do meio em que se encontram, devendo ser protegidos contra divulgação, modificações, remoção ou destruição não autorizada;

5.4.6. As pessoas que possuem acesso aos ativos da IMBEL devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação; e

5.4.7. Os processos e atividades que sustentam os serviços críticos disponibilizados pela IMBEL devem ser protegidos de forma a garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações e comunicações.

5.5. **Gestão da Continuidade do Negócio:**

5.5.1. A Estrutura de SIC da IMBEL, em conjunto com as áreas responsáveis pelos ativos da empresa, deverão instituir normas, procedimentos e controles que estabeleçam a gestão de continuidade do negócio, a fim de minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços da empresa; e

5.5.2. A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional da IMBEL.

5.6. **Auditoria e Conformidade:**

5.6.1. Consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação;

5.6.2. É facultado o acesso do Administrador da Rede local a todos os equipamentos de TIC, mesmo os eventuais particulares que estiverem logados à Rede de Dados, quando autorizados, de forma a viabilizar o procedimento de auditoria, controle e segurança que se fizer necessário;

5.6.3. A implantação e manutenção da rede de dados da IMBEL (Sede/Brasília e Unidades de Produção) serão realizadas de forma descentralizada, sob a responsabilidade da área de TIC, da Sede/Brasília e das UP, cabendo à CGTIC a auditoria da rede, quando necessário;

5.6.4. Garantir segurança especial para os sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

5.6.5. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;

5.6.6. Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

5.6.7. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros;

5.6.8. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado:

5.6.8.1. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;

5.6.8.2. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; e

5.6.8.3. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

5.7. **Controles de Acesso:**

5.7.1. A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede;

5.7.2. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade;

5.7.3. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela

administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter;

5.7.4. No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter;

5.7.5. O uso de qualquer software de proxy com o intuito de burlar as regras de controle de acesso à Internet da IMBEL, são proibidos; e

5.7.6. Os locais onde estiverem os ativos de TIC e informações classificadas deverão ser considerados como áreas restritas. Os responsáveis por essas áreas deverão providenciar controle de acesso físico específico.

5.8. **Uso de e-mail:**

5.8.1. Propriedade dos bens: serão considerados de propriedade da IMBEL todos os arquivos e softwares instalados oficialmente ou armazenados nos meios de TI pertencentes à instituição, desde que não violem disposições em contrário; inclusive o correio eletrônico (e-mail): ferramenta esta que possibilita a transferência de mensagens e qualquer outro documento eletrônico, para fins de comunicação;

5.8.2. É proibido a utilização de qualquer conta de e-mail, que não sejam as coorporativas, para a tramitação de assuntos referentes ao serviço;

5.8.3. É proibido a utilização das contas de e-mail funcionais em cadastro de sítios duvidosos na Internet. Se necessário, manter uma conta em provedor público (Gmail, Yahoo!, Hotmail, etc.) para esta finalidade (evitar a propagação de spam);

5.8.4. As contas de e-mail que não forem acessadas dentro do período de 30 (trinta) dias serão automaticamente bloqueadas;

5.8.5. O usuário deverá salvaguardar efetuar cópia de segurança/backup, dos seus arquivos pessoais e caixas de e-mail, localmente no dispositivo pessoal de trabalho e os arquivos funcionais no servidor de arquivos; e

5.8.6. Aplicam-se às transferências de mensagens efetuadas por e-mail os critérios de classificação em termos de valor, requisitos legais, sensibilidade e criticidade para a Instituição.

5.9. **Acesso a Internet:**

5.9.1. Monitorar o ambiente de TI, gerando indicadores e históricos de tempo de resposta no acesso à internet e aos sistemas críticos;

5.9.2. Monitorar períodos de indisponibilidade no acesso à internet e aos sistemas críticos;

5.9.3. Colaboradores com acesso à internet não poderão efetuar upload (subir) de qualquer software licenciado ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados;

5.9.4. Os colaboradores com acesso à internet poderão fazer o download (baixar) somente de programas ligados diretamente às suas atividades, devendo solicitar a área de TIC autorização para realização de tal ato; e

5.9.5. Os computadores com assuntos sensíveis não terão acesso à Internet.

5.10. **Comitê Gestor de Segurança da Informação (CGSI):**

5.10.1. Fica instituído o Comitê Gestor da Segurança da Informação (CGSI), com atribuição de assessorar a Presidência da IMBEL nas atividades relacionadas à segurança da informação;

5.10.2. O Comitê será composto por um representante titular e respectivos suplentes indicados pelos seguintes órgãos:

5.10.2.1. Coordenadoria-Geral de Tecnologia da Informação, que o coordenará;

5.10.2.2. Diretorias;

5.10.2.3. Unidades de Produção;

5.10.2.4. Assessorias; e

5.10.2.5. Gabinete da Sede.

5.10.3. Os membros do Comitê serão indicados pelos titulares dos órgãos mencionados anteriormente, no prazo de dez dias, contados da data de publicação desta Política, e serão designados em Portaria da Presidência da IMBEL, no prazo de vinte dias, contados da data de publicação desta POSIC;

5.10.4. Os membros titulares do Comitê serão substituídos pelos respectivos suplentes, em suas ausências ou impedimentos;

5.10.5. A participação no Comitê será considerada prestação de serviço público relevante, não remunerado;

5.10.6. No prazo de noventa dias, contado da data de publicação desta Política, será aprovado regimento interno para dispor sobre a organização e o funcionamento do Comitê;

5.10.7. O Comitê se reunirá, em caráter ordinário, semestralmente e, em caráter extraordinário, por convocação de seu Coordenador.

6. PENALIDADES

6.1. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes;

6.2. O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e Comunicações (POSIC) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor; e

6.3. O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar a IMBEL, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1. **Vice-Presidente Executivo:**

7.1.1. Compete ao Vice-Presidente Executivo, nos temas relacionados à segurança da informação, assessorado pelo Comitê Gestor da Segurança da Informação:

7.1.1.1. Instituir o Comitê Gestor da Segurança da Informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à POSIC; e

7.1.1.2. Aprovar diretrizes, estratégias, normas e recomendações;

7.2. **Gestor de Segurança da Informação:**

7.2.1. O Chefe da CGTIC será o Gestor de Segurança da Informação da Empresa, competindo-lhe:

7.2.2. Promover cultura de segurança da informação e comunicações;

7.2.3. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

7.2.4. Fiscalizar a execução das ações da POSIC de responsabilidade das Diretorias, Unidades de Produção e Gabinete da IMBEL;

7.2.5. Propor recursos necessários às ações de segurança da informação e comunicações;

7.2.6. Coordenar o Comitê Gestor de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

7.2.7. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

7.2.8. Implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidas na legislação vigente;

7.2.9. Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito da IMBEL.

7.3. **Comitê Gestor de Segurança da Informação e Comunicações (CGSIC):**

7.3.1. Assessorar na implementação das ações de SIC;

7.3.2. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

7.3.3. Instituir Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas à incidentes de segurança em rede de computadores;

7.3.4. Propor alterações na POSIC; e

7.3.5. Propor Normas Internas (NI).

7.4. **Operadores e/ou detentores das estações de trabalho:**

7.4.1. Fiscalizar a aplicação e zelar pelo cumprimento dessa Política;

7.4.2. O uso dos recursos de TIC disponibilizados (Estações de Trabalho, programas/softwares e dos serviços de Correio Eletrônico, Internet, Intranet, etc) é de

responsabilidade do usuário e deve manter afinidade exclusiva com o objeto de seu contrato de trabalho ou de prestação de serviços;

7.4.3. Ao ser contratado ou se apresentar para trabalhar na IMBEL, o empregado, civil ou militar, deverá tomar conhecimento desta Política e das recomendações da área de TIC, assinando o respectivo "Termo de Responsabilidade" disponibilizado pela área de Recursos Humanos da empresa;

7.4.4. O usuário é responsável pela segurança dos ativos e processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, tais como: crachá, token, login, senha eletrônica, certificado digital e endereço de correio eletrônico; e

7.4.5. Para a cessão de informação da IMBEL a terceiros, o titular da unidade administrativa, ouvida a área jurídica da empresa, providenciará a documentação formal relativa a essa cessão.

8. DIVULGAÇÃO DA POSIC

8.1. A POSIC e suas atualizações deverão ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e terceirizados que habitualmente trabalham na IMBEL ou nas Unidades de Produção.

8.2. Os canais de divulgação da POSIC serão a Intranet, Internet, devendo, ainda, ficar disponível em locais de fácil acesso junto aos Recursos Humanos e à Comunicação Social da IMBEL e das UP.

9. ATUALIZAÇÃO DA POSIC

9.1. A SIC, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos;

9.2. Os instrumentos normativos gerados a partir desta POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal ou conforme os seguintes critérios:

9.2.1. Política de Segurança da Informação e Comunicações (POSIC):

9.2.1.1. Nível de Aprovação: Conselho de Administração da IMBEL;

9.2.1.2. Periodicidade de Revisão: Anual.

9.2.2. Normas Internas (NIs):

9.2.2.1. Nível de Aprovação: Comitê Gestor de Segurança da Informação e Comunicações (CGSIC); e

9.2.2.2. Periodicidade de Revisão: anual.

9.3. As Unidades da IMBEL poderão, a contar da publicação desta Política apresentar ao Comitê Gestor de Segurança da Informação e Comunicações, proposta de atualização e ou melhorias desta Política.

10. DISPOSIÇÕES FINAIS

10.1. A Presidência da IMBEL poderá expedir atos complementares necessários à aplicação desta POSIC;

10.2. O não cumprimento dos requisitos previstos nesta POSIC e das Normas Internas de Segurança da Informação acarretará violação aos documentos orientadores e normativos da Empresa e sujeitará o empregado às medidas administrativas e legais cabíveis;

10.3. Assim como a ética, a segurança da informação deve ser entendida como parte fundamental da cultura interna do Sistema IMBEL. Incidentes relacionados à Segurança da Informação serão encarados como contrários à ética e aos bons costumes da Empresa;

10.4. A IMBEL, pela natureza de sua função empresarial, detém dados e informações de interesse da segurança nacional, cuja divulgação não autorizada ou prematura pode gerar desvantagem competitiva ao País no mercado ou causar danos financeiros à Empresa;

10.5. Independentemente da adoção de outras medidas, o titular da Unidade Administrativa deverá, de imediato, comunicar todo incidente de SIC que ocorra no âmbito de suas atividades à CGTIC ou às secções de informática das fábricas, mediante o envio de relatório circunstanciado;

10.6. O equilíbrio entre a funcionalidade dos diversos setores da IMBEL e as restrições impostas pelas normas de segurança é impositivo para todo planejamento de segurança;

10.7. É de propriedade da Empresa, todos os "*designs*", criações ou procedimentos desenvolvidos por qualquer empregado durante o curso do seu vínculo empregatício com a IMBEL, nos termos do seu contrato de trabalho;

10.8. Todos os usuários da IMBEL são responsáveis pelas ações de SIC, observando de forma específica as atribuições pertinentes a cada cargo e /ou função; e

10.9. Os casos omissos e as dúvidas surgidas na aplicação desta POSIC serão analisados, dirimidos ou solucionados pelo Comitê Gestor de Segurança da Informação e Comunicações (CGSIC/IMBEL).

11. VIGÊNCIA

11.1. Esta POSIC entra em vigor na data de sua publicação.

O documento original encontra-se na CGTIC, devidamente assinada.