INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL

"Vinculada ao Ministério da Defesa por intermédio do Comando do Exército"

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC)

O original deste documento encontra-se arquivado no NNC/APG

Aprovada pela Diretoria Executiva da IMBEL,
na 781ª Reunião de Diretoria, de 10 de setembro de 2025.

Aprovada pelo Conselho de Administração da IMBEL,
na 393ª Reunião Ordinária, de 18 de novembro de 2025.
(Resolução nº 44/2025-CA/IMBEL, de 18 de novembro de 2025).

Brasília – Distrito Federal, 18 de novembro de 2025.

www.imbel.gov.br

HISTÓRICO DO DOCUMENTO

APROVAÇÃO		
Versão	**Diretoria-Executiva**	**Conselho de Administração**
00	617ª Reunião Ordinária (29/10/2019)	325ª Reunião Ordinária (18/12/2019)
01	781ª Reunião Ordinária (10/09/2025)	393ª Reunião Ordinária (18/11/2025)

SUMÁRIO

1 IDENTIFICAÇÃO GERAL DA EMPRESA 3
2 FINALIDADE 4
3 REFERÊNCIAS 4
4 DISPOSIÇÕES GERAIS 5
5 OBJETIVO.....6
6 PRINCÍPIOS 7
7 DIRETRIZES GERAIS.....7
8 PROPRIEDADE DA INFORMAÇÃO.....8
9 CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO 9
10 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E REDE....10
11 GERENCIAMENTO DE RISCOS 10
12 COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO 10
13 GESTÃO DE CONTINUIDADE DE NEGÓCIO 12
14 MONITORAMENTO, AUDITORIA E CONFORMIDADE.....12
15 CONTROLE DE ACESSO E USO DE SENHAS.....12
16 ACESSO A INTERNET, USO DO *E-MAIL* E OUTROS RECURSOS.....13
17 GESTÃO DE ATIVOS 13
18 SEGURANÇA FÍSICA DOS EQUIPAMENTOS 13
19 SERVIÇOS TERCEIRIZADOS 14
20 USO, AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMA DE INFORMAÇÃO.....14
21 USO DA INTELIGÊNCIA ARTIFICIAL – IA 14
22 GESTÃO DE SEGURANÇA NA COMUNICAÇÃO 14
23 PROTEÇÃO DE DADOS PESSOAIS 15
24 COMPETÊNCIAS E RESPONSABILIDADES 15
25 PENALIDADES 16
26 DIVULGAÇÃO DA POSIC 16
27 ATUALIZAÇÃO DA POSIC.....16
28 DISPOSIÇÕES FINAIS 17
29 GLOSSÁRIO 18

1 IDENTIFICAÇÃO GERAL DA EMPRESA

EMPRESA PÚBLICA: INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL – IMBEL
CNPJ: **.444.232/0001-**
NIRE: 5350000027-5
Sede: Brasília, Distrito Federal.
Tipo de estatal: empresa pública dependente.
Acionista controlador: União.
Tipo societário: não definido.
Tipo de capital: fechado.
Abrangência de atuação: nacional e internacional.
Setor de atuação: defesa e segurança.
Diretor Administrativo-Financeiro: Marcio Gabriel Ribeiro (61) 2035-4440 marcio.ribeiro@imbel.gov.br

AUDITOR INDEPENDENTE
METROPOLE - AUDITORES INDEPENDENTES ASSOCIADOS.
Endereço: Setor de Rádio e Televisão Norte (SRTVN) – Quadra 701 – Conjunto C – Bloco B – Sala 519 – Centro Empresarial Norte – Asa Norte, Brasília, Distrito Federal.
Telefone: (61) 3326 – 6563.
Responsável Técnico: Fábia Marques Braga (CRC ***.977-**).

CONSELHO DE ADMINISTRAÇÃO DA IMBEL – CA		
REPRESENTANTES	**CONSELHEIROS**	**CPF**
Presidente do CA - Comando do Exército	Gen Ex **HERTZ** Pires do Nascimento	***.124.147-**
Diretor-Presidente da IMBEL	Gen Div R/1 Ricardo Rodrigues **CANHACI**	***.110.607-**
Ministério da Fazenda	Fernanda Garcia Machado	***.919.778-**
Ministério da Gestão e Inovação	Rodrigo Estrela de Carvalho	***.840.857-**
Ministério da Defesa	Eduardo Cesar Pasa	***.035.920-**
Ministério da Defesa	Ricardo de Mello Araujo	***.772.961-**
Empregados da IMBEL	Benedito Raimundo Venancio	***.672.926-**

DIRETORIA-EXECUTIVA DA IMBEL – DIREX		
CARGO	**DIRETORES**	**CPF**
Diretor-Presidente	Gen Div R/1 Ricardo Rodrigues **CANHACI**	***.110.607-**
Vice-Presidente Executivo	Gen Bda R/1 João **DENISON** Maia Correia	***.509.727-**
Diretor de Inovação	Cel R/1 **THIERS** Lobo Ribeiro	***.566.118-**
Diretor Administrativo-Financeiro	Cel R/1 Marcio **GABRIEL** Ribeiro	***.131.897-**
Diretor Industrial	Cel R/1 André Luiz de **ASSIS** Miranda	***.616.004-**
Diretor Comercial	Cel R/1 Eduardo Rangel de **CARVALHO**	***.047.307-**

2 FINALIDADE

Essa política tem por finalidade estabelecer diretrizes e responsabilidades que devem nortear as atividades corporativas quanto a proteção às informações contra ameaças a sua integridade, disponibilidade e confiabilidade na IMBEL. Abrange todos os níveis e setores de atuação, inclusive parceiros e colaboradores externos.

3 REFERÊNCIAS

3.1 Decreto-Lei n° 5.452, de 1/05/1943, que aprova a Consolidação das Leis do Trabalho (CLT);

3.2 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000: gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2018.

3.3 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001: segurança da informação, segurança cibernética e proteção da privacidade: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2022.

3.4 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: segurança da informação, segurança cibernética e proteção da privacidade: controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

3.5 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27005: segurança da informação, segurança cibernética e proteção da privacidade: orientações para a gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2023.

3.6 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 42001: tecnologia da informação: inteligência artificial: sistema de gestão. Rio de Janeiro: ABNT, 2024.

3.7 BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Dispõe sobre a Política Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União: seção 1, Brasília, DF, 2018.

3.8 BRASIL. Decreto nº 10.748, de 16 de julho de 2021. Institui o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP. Diário Oficial da União: seção 1, Brasília, DF, 2021.

3.9 BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. Diário Oficial da União: seção 1, Brasília, DF, 2025.

3.10 BRASIL. Gabinete de Segurança Institucional. Instrução Normativa nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Brasília, DF: GSI/PR, 2020.

3.11 BRASIL. Gabinete de Segurança Institucional. Instrução Normativa nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. Brasília, DF: GSI/PR, 2021.

3.12 BRASIL. Gabinete de Segurança Institucional. Instrução Normativa nº 5, de 30 de agosto de 2021. Dispõe sobre os requisitos mínimos de segurança da informação para contratação de soluções de computação em nuvem. Brasília, DF: GSI/PR, 2021.

3.13 BRASIL. Gabinete de Segurança Institucional. Instrução Normativa nº 6, de 23 de dezembro de 2021. Estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal. Brasília, DF: GSI/PR, 2021.

3.14 BRASIL. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 20/IN01/DSIC/GSIPR, de 15 de dezembro de 2014. Estabelece diretrizes de Segurança da Informação e Comunicações para processos de tratamento da informação na Administração Pública Federal, direta e indireta. Brasília, DF: GSI/PR, 2014.

3.15 BRASIL. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 14/IN01/DSIC/GSIPR. Portaria nº 9, de 15 de março de 2018. Estabelece princípios, diretrizes e responsabilidades relacionado à segurança da informação para o tratamento da informação em ambiente de computação em nuvem na Administração Pública Federal, direta e indireta. Brasília, DF: GSI/PR, 2018.

3.16 BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Diário Oficial da União: seção 1, Brasília, DF, 2011.

3.17 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 2018.

3.18 BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Diário Oficial da União: seção 1, Brasília, DF, 2021.

3.19 BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Padrões de Interoperabilidade de Governo Eletrônico (ePING). Versão 2024. Brasília, DF, 2024. Disponível em: https://www.gov.br/governodigital. Acesso em: nov. 2025.

3.20 INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL. 00.N.T-001: Segurança de Tecnologia da Informação – Normas de Procedimentos. Rev. 01. Brasília, DF: IMBEL®, 2022.

4 DISPOSIÇÕES GERAIS

4.1 A Política de Segurança da Informação e Comunicações (POSIC) declara o comprometimento da alta direção da IMBEL® com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a Gestão de Segurança da Informação e Comunicações (GSI) na Empresa.

4.2 Para os efeitos desta Política, entende-se como “IMBEL®”, as seguintes unidades: A IMBEL SEDE, estabelecida em Brasília (DF), a Fábrica Estrela (FE), estabelecida na cidade de Magé (RJ), a Fábrica de Itajubá (FI), estabelecida na cidade de Itajubá (MG), a Fábrica Presidente Vargas (FPV), estabelecida na cidade de Piquete (SP), a Fábrica de Juiz de Fora (FJF), estabelecida na cidade de Juiz de Fora (MG), a Fábrica de Material de Comunicações e Eletrônica (FMCE), estabelecida na cidade de Rio de Janeiro (RJ) e a Rede Elétrica Piquete-Itajubá (REPI), estabelecida na cidade de Wenceslau Braz (MG).

4.3 A POSIC aplica-se a todas as Unidades, Administrativas e de Produção, 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.

4.4 A POSIC tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

4.5 Fica instituída a 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.

4.6 A Assessoria de Gestão da Tecnologia da Informação e Comunicações (AGTIC) é responsável pela elaboração, atualização e manutenção da Política de Segurança da Informação e Comunicações (POSIC), bem como pela criação, integração e coordenação dos planos complementares atualmente vigentes e daqueles que venham a ser instituídos futuramente, conforme as necessidades da área de Tecnologia da Informação e Comunicações (TIC).

4.7 Sempre que necessário, a AGTIC poderá propor e instituir planos específicos com o objetivo de atender normativos internos ou externos, ou ainda para assegurar a conformidade com exigências legais, regulatórias ou de boas práticas relacionadas à segurança da informação, governança digital e proteção de dados.

5 OBJETIVO

Estabelecer diretrizes, regras, objetivos e valores a serem adotados na Gestão da Segurança da Informação e Comunicação (GSIC), no âmbito da IMBEL®, de acordo com sua missão e com as leis e regulamentações relevantes ao caso. Para tanto, deve atender às seguintes orientações:

a) Estabelecer uma política clara e alinhada com a missão da IMBEL®, que é a de promover soluções em Defesa e Segurança fortalecendo as suas Capacidades Estratégicas e a Soberania Nacional;

b) Assegurar o suporte e dedicação à segurança da informação por meio da promoção, atualização e manutenção da POSIC;

c) Revisar as diretrizes de segurança da informação, a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia;

d) Orientar procedimentos de manuseio, tratamento, controle e proteção de dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio, ou recurso da IMBEL® evitando ameaças e vulnerabilidades;

e) Preservar a imagem institucional da IMBEL®, bem como seus ativos de informação;

f) Fornecer orientações sobre a gestão e o tratamento de riscos relacionados a Incidentes de Segurança da Informação e Comunicação (SIC), conforme as normas regimentais;

g) Fomentar a formação e a qualificação dos gestores de segurança da informação;

h) Difundir na IMBEL® a cultura da segurança da informação; e

i) Apoiar e contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio de ações de segurança da informação, em conformidade com a Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709, de 14 de agosto de 2018.

6 PRINCÍPIOS

6.1 A segurança da informação visa diminuir riscos como vazamentos, fraudes, erros e uso indevido dos ativos da Empresa. Busca prevenir sabotagens, paralisações, roubo de dados e outras ameaças prejudiciais aos sistemas de conhecimento, recursos de processamento ou equipamentos organizacionais.

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

6.3 Visão abrangente e sistêmica da segurança da informação.

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

6.5 Preservação do acervo histórico da IMBEL®.

6.6 Educação é o alicerce fundamental para o fomento da cultura em segurança da informação.

6.7 Orientação à gestão de riscos e à gestão da segurança da informação.

6.8 Prevenção e tratamento de incidentes de segurança da informação.

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

6.10 Dever dos órgãos, das entidades e dos agentes públicos é 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.

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

7 DIRETRIZES GERAIS

7.1 Na IMBEL, os usuários deverão usar os recursos de processamento de informações fornecidos pela Empresa para garantir a segurança necessária na execução de suas atividades.

7.2 As autorizações de acesso aos recursos de processamento de informação serão concedidas pelos chefes e responsáveis pelas unidades organizacionais da empresa.

7.3 Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se de informações, de forma não autorizada.

7.4 O cumprimento da POSIC será auditado pela Auditoria Interna da IMBEL®, com a assessoria do CGSIC.

7.5 Os recursos de processamento de dados disponibilizados aos usuários terão suporte de um Plano de Prevenção de Riscos, de acordo com a norma de Gestão de Riscos em segurança de dados, a fim de evitar situações de risco à proteção desses dados.

7.6 Quaisquer recursos de processamento da informação serão testados em ambiente de homologação antes de serem colocados em produção, de acordo com norma de Aquisição, Desenvolvimento e Manutenção de Sistemas.

7.7 Os empregados da IMBEL estão sujeitos à POSIC e têm o dever de observar integralmente o disposto. A inobservância dessa política acarretará penalidades previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

7.8 Não é dado ao empregado o direito de alegar desconhecimento da POSIC, devendo este seguir rigorosamente o proposto. O desconhecimento desta política por parte do usuário não o isenta das responsabilidades e penalidades previstas.

7.9 É condição para acesso aos ativos de informação da IMBEL a adesão formal aos termos desta Política. (não acatado o parecer, para acesso aos ativos a empresa é obrigada a aceitar tal termo de adesão).

7.10 O agente público da IMBEL é responsável pela segurança dos ativos de informação e processos que estejam sob sua responsabilidade.

7.11 Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pela IMBEL serão utilizados estritamente para seu propósito.

7.12 É vedado, a qualquer colaborador e agente público da IMBEL®, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem desta entidade, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

7.13 Todos os empregados da IMBEL devem seguir rigorosamente os Planos de Tecnologia decorrentes dessa Política.

8 PROPRIEDADE DA INFORMAÇÃO

8.1 Informação é patrimônio - toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela IMBEL é considerada parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade.

8.2 Toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelos colaboradores e agentes públicos da IMBEL®, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e nas regulamentações em vigor, conforme a classificação das informações, sem prejuízo da autoria, conforme definido em lei e de acordo com a norma de Classificação da Informação.

8.3 Quando da obtenção de informação de terceiros, o gestor da informação providenciará, junto à concedente, a documentação formal atinente aos direitos de acesso, antes de seu uso, conforme norma complementar em seu sistema de classificação da informação (SCI).

8.4 Na transferência de bases de dados nominais custodiadas ou no conhecimento de propriedade da IMBEL® a terceiros, o gestor dos dados providenciará a documentação formal relativa à autorização de acesso aos detalhes, conforme norma complementar em seu SCI, excetuando os casos previstos em lei;

8.5 Procedimentos adequados asseguram a conformidade com requisitos legislativos, regulamentares e contratuais no uso de materiais. Estes podem conter direitos de propriedade intelectual. Adicionalmente, o uso de produtos de softwares proprietários segue a norma de aquisição, desenvolvimento e manutenção de sistemas.

8.6 Privacidade e a proteção de dados que esteja em conformidade com as exigências das legislações relevantes, regulamentações e cláusulas contratuais de acordo com a norma de proteção de dados pessoais.

9 CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

9.1 A classificação e o tratamento da informação observarão os seguintes requisitos e critérios:

a) O valor, requisitos legais, sensibilidade e criticidade da informação para o IMBEL; e

b) Conjunto apropriado de procedimentos para rotulação e tratamento da informação, que será definido e implementado conforme os critérios adotados pela IMBEL.

9.2 A classificação e o tratamento de informação serão:

a) Norteadas pela legislação específica, que disponha sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (APF);

b) Implementados e mantidos, em conformidade com a legislação vigente, visando a estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade da IMBEL, ao longo do seu ciclo de vida; e

c) Realizados de acordo com norma específica de classificação da informação.

9.3 As informações geridas pela IMBEL serão protegidas de maneira adequada contra acesso e uso não autorizados. Para aquelas consideradas de alta criticidade, serão necessárias medidas especiais de tratamento de acordo com a norma de classificação da informação.

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

9.5 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.

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

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

9.8 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.

9.9 A informação deve ser salvaguardada baseando-se em seu valor, sensibilidade e criticidade através de um sistema de classificação apropriado.

10 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E REDE

10.1 O processo de gestão de incidentes de segurança da informação consiste em um conjunto de práticas e procedimentos adotados pela IMBEL® para lidar com ataques ou violações que possam comprometer seus sistemas, redes ou dados, inclusive dados pessoais

10.2 A Gestão de Incidentes de Segurança da Informação e Comunicação deve identificar, monitorar, comunicar e tratar, em tempo hábil, os incidentes, de forma a garantir a continuidade das atividades da IMBEL®, sem prejuízo de sua comunicação à SIC.

11 GERENCIAMENTO DE RISCOS

11.1 As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da IMBEL.

11.2 A abordagem de gestão de riscos deverá alinhar-se com a Política e o Plano de Gestão de Riscos da IMBEL.

11.3 O gerenciamento de riscos incluirá a definição preliminar do contexto, a análise e avaliação dos riscos, o plano de tratamento, a aceitação, a implementação do plano de tratamento, o monitoramento e a análise crítica, a melhoria do processo de gestão e a comunicação dos riscos.

11.4 O processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) estará alinhado à metodologia denominada PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, de 13 de outubro de 2008, de modo a fomentar sua melhoria contínua.

11.5 A gestão dos riscos em SIC terá como objetivo identificar as necessidades da IMBEL em relação aos requisitos de Segurança da Informação e Comunicação, bem como criar um sistema eficaz de Gestão de Segurança da Informação.

11.6 A gestão dos riscos em SIC seguirá os procedimentos definidos na Norma Complementar 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

12 COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

12.1 O Comitê Gestor da Segurança da Informação (CGSIC) tem como atribuição assessorar a Presidência da IMBEL® nas atividades relacionadas à Segurança da Informação. Será composto por um representante titular e o respectivo suplente, indicados pelas Diretorias, Assessorias, Unidade de Administração e Unidades de Produção, sendo designados em ato do Vice-Presidente Executivo por meio de Portaria. Reunir-se-á, em caráter ordinário, semestralmente e, em caráter extraordinário, por convocação de seu coordenador (Chefe da AGTIC).

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

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

a) Coordenadoria-Geral de Tecnologia da Informação, que a coordenará;

b) Diretorias;

c) Unidades de Produção;

d) Assessorias; e

e) Unidade de Administração (UA).

12.4 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.

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

12.6 A participação no Comitê será considerada prestação de serviço público relevante, não remunerada.

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

12.8 O Comitê se reunirá, em caráter ordinário, semestralmente e, em caráter extraordinário, por convocação de seu Coordenador (Chefe da AGTIC).

12.9 São competências do Comitê Gestor de Segurança da Informação e Comunicação:

a) Assessorar na implementação das ações de SIC;

b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

c) Instituir a ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores;

d) Propor alterações na POSIC; e

e) Propor Normas Internas (NI).

12.10 São competências atribuídas aos usuários de recursos de TIC pertencentes ou controlados pela IMBEL:

a) Conhecer e cumprir a POSIC;

b) Dentro das instalações da IMBEL®, portar crachá de identificação de maneira visível e/ou uniforme para os cargos que o exigirem;

c) Manter sigilo e trocar periodicamente a senha pessoal;

d) Zelar pelas informações e equipamentos disponibilizados para a execução do seu serviço;

e) Ao tomar conhecimento de qualquer incidente de segurança da informação, notificar o fato, imediatamente, ao CGSIC; e

f) Participar de eventos promovidos pelo CGSIC relacionados à segurança da informação.

13 GESTÃO DE CONTINUIDADE DE NEGÓCIO

13.1 A IMBEL deverá estabelecer procedimentos a serem seguidos para minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades, além de recuperar perdas de ativos de informação em um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

13.2 Toda informação institucional deverá ser mantida em local que a salvaguarde adequadamente.

13.3 Deverá ser mantida uma estrutura básica de planos de continuidade de operações e serviços, para assegurar consistência, para contemplar os requisitos de segurança da informação e identificar prioridades de testes e manutenção.

14 MONITORAMENTO, AUDITORIA E CONFORMIDADE

14.1 A avaliação técnica de conformidade em Segurança da Informação e Comunicação deverá considerar a POSIC com suas normas e os requisitos legais pertinentes.

14.2 A avaliação de conformidade em SIC deverá ser aplicada de forma contínua, visando contribuir para a Gestão de Segurança da Informação e Comunicação do GSI.

14.3 É facultado o acesso do Administrador da Rede local da rede de dados a todos os equipamentos de TIC, mesmo os eventuais particulares que estiverem logados à Rede de Dados, quando autorizados pela AGTIC, de forma a viabilizar o procedimento de auditoria, controle e segurança.

14.4 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 AGTIC a auditoria da rede, quando necessário.

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

14.6 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.

14.7 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.

14.8 Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação de superiores, ou por determinação do CGSIC.

15 CONTROLE DE ACESSO E USO DE SENHAS

15.1 O controle de acesso e uso de senhas visa contribuir para a garantia da integridade, disponibilidade, confidencialidade e autenticidade das informações da IMBEL.

15.2 As regras específicas do controle de acesso e senhas do ambiente IMBEL serão estabelecidas pela IMBEL, obedecendo às boas práticas utilizadas no mercado.

16 ACESSO A INTERNET, USO DO *E-MAIL* E OUTROS RECURSOS

16.1 A IMBEL proporcionará aos seus empregados, a quem assim necessitar para o desempenho do seu laboro diário, acesso a internet, *e-mail* e demais recursos necessários.

16.2 As regras específicas do uso da internet, e-mail e demais recursos de TI no ambiente IMBEL serão estabelecidas pela IMBEL obedecendo às boas práticas utilizadas no mercado.

16.3 Regras específicas de operação dos recursos acima citados no âmbito IMBEL® serão definidas em norma complementar interna.

17 GESTÃO DE ATIVOS

A gestão de ativos deverá observar:

a) Normas e procedimentos instituídos pela SIC a fim de garantir a adequada gestão dos ativos da empresa, em conjunto com as unidades responsáveis;

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

c) Medidas de segurança específicas devem assegurar a proteção apropriada dos ativos, em níveis que correspondam à sua importância para o alcance das metas e estratégias da empresa;

d) 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

e) 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.

18 SEGURANÇA FÍSICA DOS EQUIPAMENTOS

A segurança física dos equipamentos obedecerá às seguintes diretrizes:

a) A área responsável pela segurança organizacional/corporativa da IMBEL® deverá implementar perímetros de segurança, a fim de garantir proteção e separação entre ambientes internos e externos;

b) As áreas seguras deverão ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso;

c) Instalações, escritórios e salas possuirão projetos de segurança física, aprovados por órgão especialista em segurança, que contemplem saídas de emergência, extintores posicionados de maneira estratégica e revisões periódicas das instalações;

d) Áreas seguras controladas pela IMBEL® possuirão procedimentos adequados de proteção, bem como diretrizes que orientem o trabalho no interior dessas áreas, conforme norma complementar a ser estabelecida; e

e) Os equipamentos que operem fora das dependências da IMBEL® estarão sujeitos à norma complementar que trate de operações externas, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da empresa.

19 SERVIÇOS TERCEIRIZADOS

Os serviços terceirizados seguirão o seguinte:

a) A IMBEL deverá, em seus relacionamentos contratuais com terceiros, definir, especificamente, quais serviços e áreas internas serão autorizados para acesso e manuseio por terceiros; e

b) Todo acesso por terceiros às informações e ativos da IMBEL só deverá ser autorizado após regular preenchimento de Termo de Responsabilidade e de Sigilo, elaborado e sob a responsabilidade do Setor de Aquisições, Licitações e de Contratos (SALC) que deverá inseri-lo no processo de contratação.

20 USO, AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMA DE INFORMAÇÃO

20.1 Caberá ao Setor de Aquisições, Licitações e de Contratos (SALC), adotar como boa prática as instruções reguladoras da Secretaria de Governo Digital/Ministério da Gestão e Inovação (SGD/MGI) que regula o processo de aquisição e contratação de bens e serviços de TI.

20.2 Regras específicas de operação e manutenção de sistemas considerados críticos à IMBEL® serão definidas em norma complementar interna.

21 USO DA INTELIGÊNCIA ARTIFICIAL – IA

21.1 A inteligência artificial (IA) é uma tecnologia poderosa que vem sendo, gradativamente, integrada aos ambientes de trabalho, com o intuito de otimizar processos e tarefas, melhorando a eficiência operacional. Convém observar que seu uso traz consigo algumas barreiras a serem transpassadas, principalmente no que tange à segurança da informação.

21.2 Seu principal objetivo é desenvolver sistemas e algoritmos capazes de simular a inteligência humana, permitindo que as máquinas realizem tarefas complexas, tomem decisões autônomas e aprendam com experiências passadas.

21.3 Regras específicas do uso da IA no ambiente IMBEL® deverão ser estabelecidas em norma complementar interna.

22 GESTÃO DE SEGURANÇA NA COMUNICAÇÃO

A gestão de segurança na comunicação seguirá as seguintes diretrizes:

a) A divulgação de informações nos meios de comunicação social, incluindo internet, estará de acordo com a norma de organização interna da segurança da informação e comunicação da POSIC;

b) As informações e símbolos institucionais do órgão somente devem ser divulgados com autorização do Presidente da IMBEL® ou gestor por ele delegado;

c) Os empregados, livremente, quando divulgar nos seus perfis pessoais das Redes Sociais (YouTube, Facebook, Instagram, WhastApp e outras), os dados, as informações, as imagens e quaisquer outras atividades de exposição, poderão fazê-lo, desde que se responsabilizem, de forma administrativa, civil e criminal pelos seus atos, que possam evidenciar ou venham caracterizar ofensa à honra e a dignidade do Empregador ou Superiores hierárquicos, ainda que seja em eventos realizados ou patrocinados pela Empresa; e

d) O empregado que vazar ou repassar, sem autorização da Empresa, informações estratégicas, operacionais, de segurança e de inteligência da IMBEL estará sujeito às sanções administrativas, cíveis e penais cabíveis.

23 PROTEÇÃO DE DADOS PESSOAIS

23.1 Os dados privados, pessoais e/ou sensíveis do titular, de crianças e adolescentes deverão ser processados de forma legal, justa e transparente em relação aos seus titulares e observarão:

a) A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018; e

b) Normativos internos da IMBEL.

23.2 A IMBEL assegurará que o tratamento de dados pessoais observe os princípios da LGPD, adotando medidas técnicas e organizacionais para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações.

23.3 Em caso de incidentes envolvendo dados pessoais, a IMBEL® seguirá os procedimentos definidos pela Equipe de Tratamento de Incidentes em Redes Computacionais (ETIR), avaliando, quando necessário, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares.

23.4 A avaliação quanto à obrigatoriedade de notificação considerará o risco ou dano relevante aos titulares, conforme critérios definidos pela ANPD.

24 COMPETÊNCIAS E RESPONSABILIDADES

24.1 A estrutura de Gestão de Segurança da Informação na IMBEL® será composta pelo Gestor de Segurança da Informação (GSIC); pelo Comitê Gestor de Segurança da Informação e Comunicação (CGSI); pela Assessoria Especial de Segurança Orgânica Corporativa (Asse Esp Seg Org Corp); pelo Encarregado de Proteção de Dados Pessoais (DPO) e pela Equipe de Tratamento de Incidentes de Redes Computacionais (ETIR).

24.2 Compete ao Vice-Presidente Executivo, referente à SIC:

a) Instituir o Comitê Gestor de Segurança da Informação e Comunicações (CGSIC), ou equivalente, para deliberar sobre os assuntos relativos à SIC; e

b) Aprovar, após deliberação do CGSIC, diretrizes, estratégias, normas e recomendações referentes à SIC na IMBEL®.

24.3 A função de Gestor de SIC na IMBEL® será desempenhada pelo Chefe da Assessoria de Gestão da Tecnologia da Informação e Comunicação (AGTIC), que terá, como competências:

a) Promover a cultura de SIC, na IMBEL®;

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança da informação;

c) Fiscalizar a execução das ações da POSIC de responsabilidade das Diretorias, Unidades de Produção e Unidade de Administração (UA);

d) Propor recursos necessários às ações de SIC na Empresa;

e) Coordenar o CGSIC e o ETIR;

f) Coordenar estudos de novas tecnologias quanto a possíveis impactos na SIC;

g) Implementar e manter mecanismos, instâncias e práticas de governança da SIC em consonância com os princípios e diretrizes estabelecidos na legislação vigente; e

h) Propor ao CGSIC, normas e procedimentos relativos à SIC no âmbito da IMBEL.

25 PENALIDADES

25.1 O uso de qualquer recurso para atividades ilícitas resultará em ações administrativas e penalidades decorrentes de processos civis e criminais. Nestes casos, a instituição colaborará de maneira efetiva com os órgãos de justiça responsáveis.

25.2 O descumprimento ou violação, pelo usuário, das regras previstas na POSIC resultará na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

25.3 O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que ocasionar à IMBEL, podendo.

26 DIVULGAÇÃO DA POSIC

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

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

27 ATUALIZAÇÃO DA POSIC

27.1 A SIC, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revisada e atualizada, com vista à melhoria contínua dos processos internos.

27.2 Os instrumentos normativos gerados por meio desta e a própria POSIC deverão ser revisados sempre que se fizer necessário, conforme situações: em função de alterações na legislação pertinente, ou de diretrizes políticas do Governo Federal, ou conforme os seguintes critérios:

a) Alteração das legislações ou diretrizes políticas, do Governo Federal;

b) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma; e

c) Acolhimento de sugestões dos usuários e colaboradores da IMBEL.

27.3 São critérios para atualização:

27.3.1 Política de Segurança da Informação e Comunicações (POSIC):

a) **Nível de Aprovação:** Conselho de Administração da IMBEL®; e

b) **Periodicidade de Revisão:** Anual.

27.3.2 Normas Internas (NI):

a) **Nível de Aprovação**: Comitê Gestor de Segurança da Informação e Comunicações (CGSIC); e

b) **Periodicidade de Revisão:** anual.

27.4 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.

28 DISPOSIÇÕES FINAIS

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

28.2 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 os envolvidos às medidas administrativas e legais cabíveis.

28.3 Assim como a ética, a segurança da informação deve ser entendida como parte fundamental da cultura interna da IMBEL. Incidentes relacionados à SIC serão classificados como contrários à ética e aos bons costumes da Empresa.

28.4 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.

28.5 Independentemente da adoção de outras medidas, o titular da UA deverá, de imediato, comunicar todo ISIC que ocorra no âmbito de suas atividades à AGTIC ou às secções de informática das UA, mediante o envio de relatório circunstanciado.

28.6 O equilíbrio entre a funcionalidade dos diversos setores da IMBEL® e as restrições impostas pelas normas de segurança são imperativos para todo planejamento de segurança.

28.7 É de propriedade da Empresa, todos os *designs*, criações ou procedimentos desenvolvidos por qualquer empregado durante o curso do seu vínculo com a IMBEL®; Todos os usuários da IMBEL são responsáveis pelas ações de SIC, observando de forma específica as atribuições pertinentes a cada cargo e /ou função.

28.8 Os casos omissos e as dúvidas surgidas na aplicação desta POSIC serão analisados, dirimidos ou solucionados pelo CGSIC.

28.9 Este documento entra em vigor a partir da data de sua publicação, revogando-se as disposições anteriores, em especial à POSIC / IMBEL®, aprovada pela Resolução nº 41/2019 CA/IMBEL, 18 de dezembro de 2019.

29 GLOSSÁRIO

Para fins da POSIC, considera-se:

29.1 **Acesso:** Ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

29.2 **Gestão de Riscos:**

a) **Análise de Risco:** é o processo de identificação e avaliação de possíveis problemas, que podem impactar negativamente o negócio;

b) **Ameaça:** Conjunto de fatores internos e externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização; e

c) **Impacto**: alteração adversa no nível de objetivos de negócio alcançados.

29.3 **Avaliação de Riscos**: Processo de comparar o risco estimado com critérios de risco predefinidos para determinar sua relevância.

29.4 **Aplicações:** Programa de computador, cujo objetivo é ajudar o seu usuário a desempenhar uma tarefa específica, em geral, ligada a processamento de dados;

29.5 **Ativo**: Tudo que tenha, ou gere, valor para a organização;

29.6 **Ciclo de Vida**: ciclo formado pelas fases da produção e recepção, organização, uso, disseminação e destinação;

29.7 **Classificação**: grau de sigilo atribuído por autoridade competente a dados, informações, documentos, materiais, áreas ou instalações;

29.8 **Comitê Gestor de Segurança da Informação e Comunicações (CGSIC):** equipe responsável por orientar a implementação de medidas de segurança de informação e comunicação na IMBEL®;

29.9 **Controle**: refere-se às medidas implementadas para proteger os ativos de informação de uma organização contra ameaças e garantir sua confidencialidade, integridade e disponibilidade;

29.10 **Evento**: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;

29.11 **Gestor de Segurança da Informação e Comunicação (GSIC)**: responsável pelas ações de segurança da informação e comunicações, no âmbito da IMBEL®;

29.12 **Incidente de Segurança da Informação e Comunicação (ISIC)**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

29.13 **Normativos e Legislações**:

a) **ISO/IEC 27001**: É uma norma internacional que define os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação e Comunicação (SGSIC) em uma organização;

b) **NIST SP 800-53 (SPECIAL PUBLICATION 800-53)**: Documento publicado pelo *National Institute of Standards and Technology* (NIST) dos Estados Unidos, compõem parte do conjunto de publicações do NIST voltado para a segurança

da informação e destina-se a fornecer diretrizes e controles de segurança para sistemas de informação e redes;

c) **Lei Geral de Proteção de Dados (LGPD)**: é a legislação brasileira aprovada em 2018 que controla a privacidade e o uso/tratamento de dados pessoais e que também altera os artigos 7º e 16º do Marco Civil da Internet; e

d) **NURTI**: **Normas** de Utilização de Recursos de Tecnologia da Informação. Tem por objetivo, dentre outros, disciplinar a utilização mais adequada dos recursos de TI da Empresa e elevar o nível de segurança da informação, estabelecendo responsabilidades dos empregados no processo;

29.14 **Núcleo de Informação e Coordenação do Ponto BR (NIC.br):** 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.

29.15 **Planos e Políticas**:

a) **Plano de Continuidade de Negócios (PCN):** documentação dos procedimentos e informações necessárias para que a organização mantenha seus ativos de informação críticos e a continuidade de suas atividades em local alternativo num nível previamente definido, em casos de incidentes;

b) Política de Segurança da Informação e Comunicações (POSIC): Conjunto de diretrizes, procedimentos e práticas estabelecidas por uma entidade, para proteger seus ativos, recursos e interesses contra ameaças internas e externas. Essas ameaças podem incluir ataques cibernéticos, intrusões físicas, desastres naturais, sabotagem, entre outros; e

c) **Plano Setorial:** Descritos dos projetos e das ações relevantes que o órgão ou Unidade Administrativa (UA) pretende realizar durante um exercício (um ano), contemplando desdobramentos do plano estratégico.

29.16 **Conhecimento:**

a) **Dados:** Conjunto de valores ainda não processados, que podem ser armazenados e manipulados para gerar informações. Eles podem ser estruturados, como em bancos de dados relacionais, ou não estruturados, como arquivos de texto ou mídia digital;

b) **Informação:** São os dados processados que podem ser utilizados para a produção de conhecimento, contidos em qualquer meio, suporte ou formato;

c) **Informação Pessoal:** informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

d) **Conhecimento:** Contextualização das informações obtidas dos dados com o intuito de direcionar as decisões estratégicas, táticas e operacionais;

e) **Sabedoria:** Conversão de conhecimento adquirido em valor, crença e cultura, visando vantagens ou benefícios.

29.17 **Princípios da Segurança da Informação:**

a) **Autenticidade**: Garantir que a informação foi enviada pelo mesmo indivíduo que se identifica como remetente;

b) **Confidencialidade**: Garantir que a informação estará acessível apenas para pessoas autorizadas;

c) **Disponibilidade**: Garantir que as informações estejam disponíveis para serem acessadas a qualquer momento pelos usuários autorizados; e

d) **Integridade:** Garantir que a informação não foi manipulada durante sua transmissão, sendo a mesma gerada na fonte que chega ao destino.

29.18 **Recursos de Processamento da Informação:** qualquer sistema de processamento da informação, serviço, infraestrutura ou as instalações físicas que os abriguem;

29.19 **Termo de Responsabilidade**: documento que estabelece, claramente, os direitos, deveres e obrigações das partes envolvidas em uma atividade ou projeto;

29.20 **Unidade Administrativa (UA):** Unidade que possui três características: pessoal, patrimônio e competências próprias, não sendo critério necessário ter orçamento para se dizer que uma unidade é administrativa; e

29.21 **Usuário**: pessoa, conta, máquina ou processo, que tem acesso a um sistema de informação.

Brasília – Distrito Federal, 18 de novembro de 2025.

General de Exército HERTZ PIRES DO NASCIMENTO
Presidente do Conselho de Administração

Gen Div R/1 RICARDO RODRIGUES CANHACI
Membro do Conselho de Administração

RODRIGO ESTRELA DE CARVALHO
Membro do Conselho de Administração

EDUARDO CESAR PASA
Membro do Conselho de Administração

FERNANDA GARCIA MACHADO
Membro do Conselho de Administração

BENEDITO RAIMUNDO VENANCIO
Membro do Conselho de Administração

RICARDO DE MELLO ARAUJO
Membro do Conselho de Administração