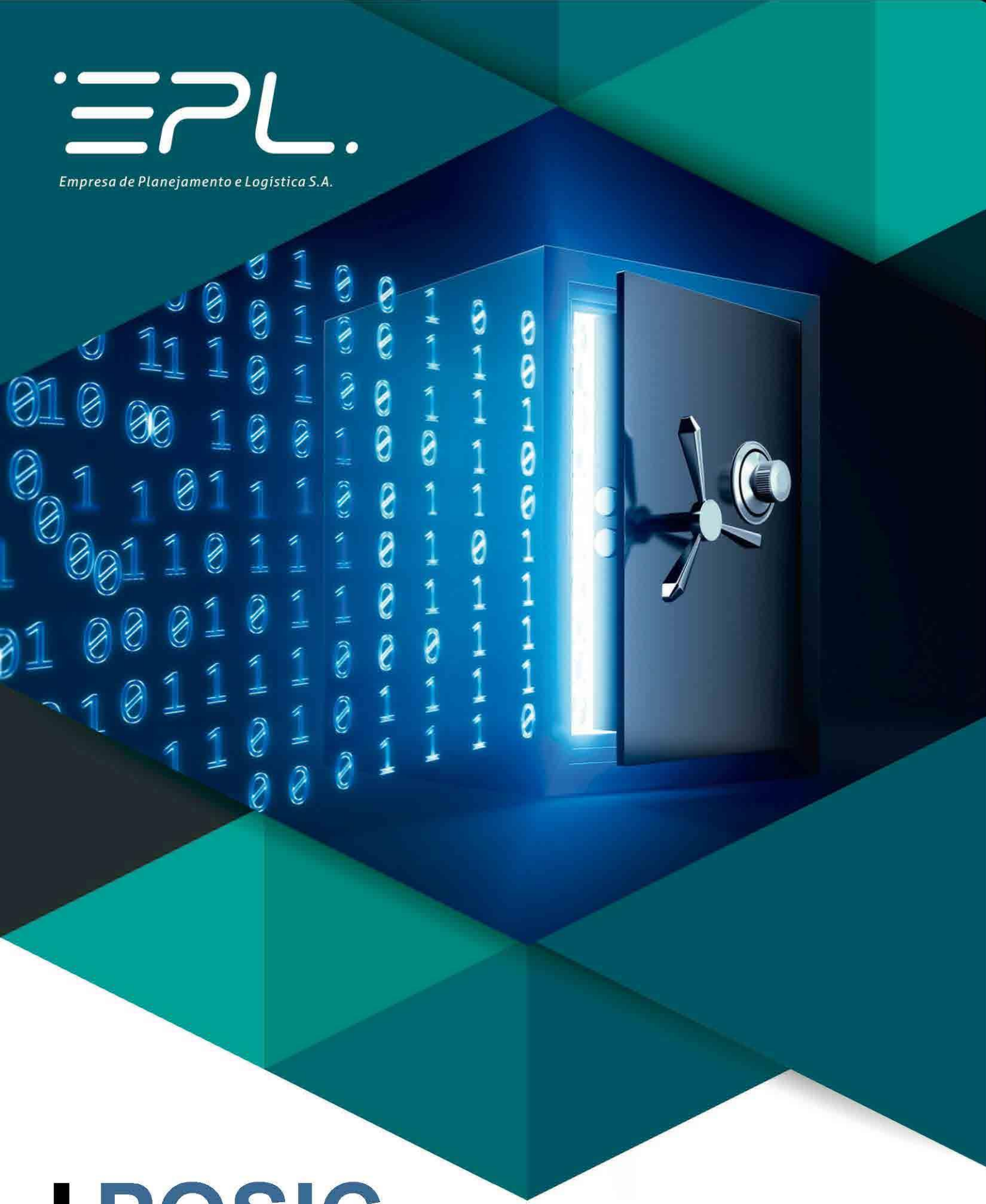
EPL.

Empresa de Planejamento e Logística S.A.



POSIC

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA EPL - PoSIC

A Empresa de Planejamento e Logística S.A. – EPL, instituida pela Lei nº 12.404 de maio de 2011 e modificada pela Lei n° 12.743, de dezembro de 2012, vinculada à Secretaria de Governo da Presidência da República, é responsável por elaborar estudos de viabilidade técnica, jurídica, ambiental e econômico-financeira necessários ao desenvolvimento de projetos de logística e transportes no País. Dando cumprimento as suas atribuições e responsabilidades, resolve:

Art. 1° Instituir a Política de Segurança da Informação e Comunicações - PoSIC da Empresa de Planejamento e Logística - EPL.

§ 1º A PoSIC tem por finalidade assegurar o tratamento adequado dos ativos de informação produzidos ou custodiados pela empresa, bem como a conservação, guarda e a proteção das informações, tendo como base as diretrizes e valores adotados pela EPL.

§ 2º Esta PoSIC se aplica a todos os agentes públicos da EPL.

CAPÍTULO I
DO OBJETIVO E ABRANGÊNCIA

Art. 2º A PoSIC tem por objetivo instituir princípios e diretrizes de Segurança da Informação e Comunicações - SIC no âmbito da EPL, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e comunicações que suportam os objetivos estratégicos da Empresa.

Parágrafo único. A PoSIC obedecerá aos valores que orientam a EPL no cumprimento dos seus objetivos, são eles: celeridade, transparência, sustentabilidade, inovação, credibilidade e valorização das pessoas.

CAPÍTULO II
DAS DEFINIÇÕES E CONCEITOS

Art. 3° Para os efeitos deste ato, considera-se:

I – acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II – agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de

investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

III – ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja por trazer danos diretos e/ou prejuízos, decorrentes de situações inesperadas;

IV – ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V – autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VI – comitê de segurança da informação e Comunicações – CSIC: instância estratégica, responsável por tratar e deliberar a respeito de temas na área de Segurança da Informação e Comunicações;

VII – controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

VIII – custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos da informação que não lhe pertence, mas que se encontra sob sua guarda ou custódia;

IX – disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

X – equipe de tratamento e respostas a incidentes em redes computacionais-ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

XI - gestão de ativos de informação: processo abrangente de gestão que inventaria e mapeia os ativos de informação institucionais, identificando, no mínimo e de forma inequívoca, seu conjunto completo de informações básicas (nome, descrição e localização), seus respectivos responsáveis (proprietários e custodiantes), seus requisitos legais e de negócio, sua classificação, sua documentação, seu ciclo de vida, seus riscos associados e seus controles de SIC implementados, bem como os outros ativos de informação relacionados;

XII – gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais à EPL, e os possíveis impactos nas operações dos negócios, caso as ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XIII – gestão de risco de segurança da informação e comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XIV – gestão de segurança da informação e comunicações – GSIC: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

XV – gestor de segurança da informação e comunicações: colaborador nomeado, para ser o responsável pela gestão da segurança da informação e comunicação, na EPL;

XVI – incidente de segurança da informação e comunicações: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XVII – informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XVIII – infraestrutura em tecnologia da informação: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes de telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XIX – integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XX – política de segurança da informação e comunicações - PoSIC: documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de fornecer diretrizes, critérios e suportes administrativos suficientes para a implementação da Segurança da Informação e Comunicações;

XXI – quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXII – segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXIII – segurança física ou do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXIV – termo de responsabilidade: termo assinado pelo usuário no qual concorda em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XXV – tratamento de incidentes: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXVI – tratamento da informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento e eliminação de controle da informação;

XXVII – usuário: empregados, prestadores de serviços, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada, para acesso aos Ativos de Informação da EPL, por meio da assinatura de Termo de Responsabilidade; e

XXVIII – vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaça.

CAPÍTULO III
DOS PRÍNCÍPIOS

Art. 4° O conjunto de documentos que compõem esta PoSIC deverá guiar-se pelos seguintes princípios de segurança da informação e comunicações:

I – segregação de função: funções de planejamento, execução e controle devem ser segregadas, de forma a atender aos objetivos institucionais e reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

II - menor privilégio: pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

III - auditabilidade: todos os eventos significantes dos processos e sistemas devem ser rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento;

IV - mínima dependência de segredos: os controles de SIC devem ser efetivos, ainda que a ameaça saiba de suas existências e do seu funcionamento;

V - controles automáticos: deverão ser utilizados, sempre que possível, controles de segurança automáticos, especialmente aqueles controles que dependem da vigilância humana e do comportamento humano;

VI - resiliência: os processos, sistemas e controles devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

VII - defesa em camadas: controles devem ser desenhados em camadas ou níveis, de tal forma que, se uma camada de controle falhar, exista um tipo diferente de controle em outra camada ou nível para prevenir a vulnerabilidade de segurança;

VIII - exceção aprovada: exceções à PoSIC devem sempre ser documentadas e ter aprovação superior; e

IX - substituição da segurança em situações de emergência: controles de segurança devem ser desconsiderados somente de formas predeterminadas e seguras, devendo existir procedimentos e controles alternativos previamente elencados para minimizar o nível de risco em situações de emergência.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 5° O modelo de GSIC da EPL deverá ser integrado e suportado pelos subsídios gerados pela Gestão de Riscos, Gestão de Ativos, Gestão de Incidentes, Gestão de Continuidade de Negócio e Gestão de Conformidade, e demais comitês institucionais criados no âmbito da EPL, em consonância com o especificado nas diretrizes desta PoSIC.

Art. 6º A GSIC deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos da EPL, assim como otimizar seus investimentos.

Art. 7º Os custos associados à GSIC deverão ser compatíveis com os custos dos Ativos que se deseja proteger.

Art. 8º As ações de GSIC devem considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, os requisitos legais, a estrutura e a finalidade da EPL.

Art. 9º A GSIC deve estabelecer critérios para a divulgação de informações de interesse público, independentemente das solicitações.

Art. 10. Os assuntos que mereçam tratamento especial deverão ser protegidos, inclusive, mediante à assinatura de Termo de Responsabilidade por todos aqueles que tenham acesso a esta informação.

Art. 11. As ações de GSIC devem considerar a realização de atividades de capacitação, criação, desenvolvimento e manutenção de uma mentalidade de segurança da informação e comunicações.

Art. 12. A GSIC será de responsabilidade de todas as unidades gerenciais da Empresa.

Art. 13. A EPL deverá observar o cumprimento desta PoSIC em todos os contratos firmados que deverão conter cláusulas que determinem a sua observância.

Art. 14. Além das diretrizes estabelecidas nesta Política, a EPL deve considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de SIC e devem estipular mecanismos que garantam a orientação à conformidade dos controles de SIC associados, inclusive sua auditabilidade.

SEÇÃO I
DA GESTÃO DE RISCOS

Art. 15. A Estrutura de SIC da EPL deverá estabelecer metodologia que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos de Tecnologia da Informação e Comunicações - TIC.

Art. 16. As unidades organizacionais da EPL, com apoio da Estrutura de SIC, deverão implementar e executar as atividades de gestão dos riscos de segurança da informação e comunicações associados aos ativos de informação sob sua responsabilidade.

Art. 17. Os riscos de SIC deverão ser considerados na contratação de serviços terceirizados, sendo os gestores das unidades organizacionais e dos ativos relacionados, 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.

Art. 18. As normas e procedimentos da EPL devem considerar controles para a troca de informações, tanto internamente quanto externamente, de forma a manter o nível adequado de segurança da informação e comunicações.

SEÇÃO II
DA GESTÃO DE ATIVOS

Art. 19. A Estrutura de SIC da EPL deve propor normas e instituir procedimentos que garantam a adequada gestão dos ativos de informação da EPL, em conjunto com as unidades organizacionais responsáveis pelos respectivos ativos.

Art. 20. Ações e controles específicos de segurança deverão garantir a proteção adequada dos ativos de informação da EPL, em níveis compatíveis ao seu grau de importância para a consecução das atividades e objetivos estratégicos da Empresa.

Art. 21. Os ativos de informação 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 autorizadas.

Art. 22. As pessoas que possuem acesso aos ativos de informação da organização devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação.

Art. 23. Os processos e atividades que sustentam os serviços críticos disponibilizados pela EPL devem ser protegidos de forma a garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações e comunicações.

SEÇÃO III
DA GESTÃO DA CONTINUIDADE DO NEGÓCIO

Art. 24. A Estrutura de SIC da EPL, em conjunto com as áreas intervenientes, responsáveis pelos ativos de informação da Empresa, deverão propor 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 dos serviços da EPL.

SEÇÃO IV
DA GESTÃO DE INCIDENTES

Art. 25. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, pela Equipe de Tratamento e Resposta a Incidentes de Rede – ETIR, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos da EPL, sem prejuízo de sua comunicação à Estrutura de SIC da EPL.

SEÇÃO V
DA CONFORMIDADE

Art. 26. O cumprimento desta PoSIC deverá ser avaliado, periodicamente, por meio de verificação de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e comunicações e garantia de cláusula de responsabilidade e sigilo.

Art. 27. Os controles de SIC devem ser analisados criticamente e verificados em períodos regulares pela Estrutura de SIC da EPL, tendo por base a conformidade com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes.

Art. 28. A Estrutura de SIC da EPL deve instituir processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Administração Pública Federal.

CAPÍTULO V
DAS DIRETRIZES ESPECÍFICAS

Art. 29. Os usuários desta PoSIC devem observar, no desenvolvimento de suas atribuições, as diretrizes abaixo estabelecidas:

I - Tratamento da Informação

a) os ativos da informação devem: i) ser inventariados e protegidos; ii) ter identificados os seus proprietários custodiantes ; iii) ter mapeado as suas ameaças, vulnerabilidades e interdependências; iv) ter a sua entrada e saída da EPL autorizadas e registradas pela autoridade competente; v) ser passível de monitoramento e ter seu uso investigado por meio de mecanismos que permitam a rastreabilidade do uso desses ativos, quando houver indício de quebra de segurança; vi) ser regulamentado por normas específicas quanto à sua utilização; e vii) ser utilizado estritamente dentro do seu propósito, observando a Lei de Acesso à Informação;

b) os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas;

c) os acessos dos usuários aos ativos de informação e sua utilização, quando autorizados, devem ser condicionados ao aceite de Termo de Responsabilidade;

d) os procedimentos para segurança e credenciamento da informação classificada devem obedecer ao Decreto n° 7.724, de 16 de maio de 2012, que regulamenta a Lei n° 12.527, de 18 de novembro de 2011, o Decreto 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e demais exigências legais;

e) o uso dos ativos da informação deve ser controlado e monitorado pela EPL, respeitando os princípios legais, para garantir a utilização estrita e correta desses recursos, bem como minimizar riscos das atividades, aos serviços e à imagem da Empresa.

II - Gestão de Risco

a) a Gestão de Risco de Segurança da Informação e Comunicações – tem como objetivo identificar os perigos, analisar, classificar e eliminar (ou mitigar) os riscos, de forma a garantir níveis aceitáveis de desempenho das atividades da EPL.

b) a Gestão de Risco de Segurança da Informação e Comunicações é um processo contínuo e deve ser aplicado para a implementação e operação da GSIC,

levando em consideração o planejamento, execução, análise crítica e melhoria da segurança da informação e da comunicação na EPL;

c) deverão ser estabelecidos normas e procedimentos, com metodologia que permita ao proprietário dos ativos da informação indicar o valor deste ativo à EPL, considerando fatores de risco aos quais possam estar expostos.

III – Segurança em Recursos Humanos

a) todo agente público em exercício na EPL deve ter ciência e firmar Termo de Responsabilidade quanto ao uso das informações utilizadas no ambiente da Empresa;

b) os usuários devem ter ciência das ameaças, responsabilidades e obrigações, bem como das preocupações da EPL referentes à segurança da informação e comunicações;

c) as atividades de ensino para capacitação dos empregados da EPL estão estruturadas em 04 (quatro) níveis: sensibilização, conscientização, capacitação e especialização em SIC;

d) todos os colaboradores da EPL serão capacitados, sendo observado o grau de envolvimento de cada indivíduo na aplicação desta PoSIC;

e) os procedimentos para controle de permissões serão estabelecidos em Normativos Específicos da segurança da informação e comunicações.

IV – Patrimônio Intelectual

a) as informações produzidas por usuários no exercício de suas funções, no âmbito da EPL, são patrimônio intelectual da organização, não cabendo a seus criadores quaisquer formas de direito autoral.

V – Controle de Acesso Físico e Lógico

a) serão estabelecidas, políticas, normas e procedimentos com o objetivo de sistematizar a concessão de acesso, visando evitar a quebra da segurança da informação e comunicações;

b) os usuários da EPL são responsáveis por todos os atos praticados com suas identificações;

c) a autorização, o acesso e o uso das informações e dos recursos computacionais

(sistemas, *e-mail, internet*) devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário;

d) todos os sistemas de informação e comunicações da EPL devem ter um gestor, formalmente designado por autoridade competente;

e) os recursos computacionais (sistemas, *e-mail, internet* e outros) disponibilizados pela EPL devem ser utilizados estritamente para o seu propósito institucional;

f) a Segurança da Informação e Comunicações da EPL deve estabelecer mecanismos de proteção às instalações físicas e às áreas de processamento de informações críticas ou sensíveis, contra acessos indevidos, danos e interferências.

VI – Gestão de Continuidade do Negócio

a) O CSIC determinará metodologias e normas para o estabelecimento da continuidade do negócio por meio da elaboração de um Plano de Gestão de Continuidade de Negócio;

b) o Processo de gestão da continuidade de negócios deverá ser implementado, mantido e testado periodicamente visando reduzir, a um nível aceitável, o tempo de interrupção causado por incidentes e acidentes de segurança que afete os ativos de informação.

VII – Tratamento de Incidentes

a) o CSIC deverá instituir metodologias e normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço normativo e técnico da gestão de segurança da informação e comunicações;

b) as alterações ou adequações da metodologia ou normas que tratem dos incidentes de segurança ocorrerão a partir dos relatórios emitidos pela Equipe de Tratamento de Respostas a Incidentes Computacionais – ETIR;

c) deverá ser estabelecido um Plano de Ação de Respostas aos Incidentes de Segurança da Informação e Comunicações, com o objetivo de interromper ou mitigar os impactos deles decorrentes.

VIII – Conformidade

a) a verificação de conformidade das práticas de segurança da informação e comunicações da EPL terá como base esta Política, suas normas e procedimentos complementares e a legislação específica;

b) aos prestadores de serviços é vedado realizar a verificação de conformidade dos próprios serviços prestados;

c) a verificação de conformidade poderá utilizar ampla variedade de técnicas, tais como análise de documentos, análise de registros, análise de código-fonte, entrevistas e testes de invasão;

d) a avaliação de conformidade em SIC deve ser contínua e aplicada visando contribuir com a gestão de segurança da informação e comunicações.

e) a conformidade das práticas de segurança da informação do Ambiente de TIC será aferida por meio de Relatório de Conformidade.

IX – Plano de Investimentos

a) os investimentos em segurança da informação e comunicações na EPL serão realizados de forma planejada e consolidados, em um Plano de Investimentos em Segurança da Informação e Comunicações;

b) o Plano de Investimentos em Segurança de Informação e Comunicações será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco;

c) o Plano de Investimentos em Segurança da Informação e Comunicações, assim como a correspondente proposta orçamentária, deverá ser aprovado pelo CSIC.

CAPÍTULO VI
DA ESTRUTURA DE SIC E SUAS RESPONSABILIDADES

Art. 30. A SIC é disciplina fundamental da boa governança corporativa, sendo de responsabilidade da alta administração da EPL.

Art. 31. Para assessorar a alta administração da EPL nas atividades de definição e implementação de diretrizes, políticas, normas e procedimentos relativos à SIC, fica instituída a Estrutura de SIC da EPL, com atribuições definidas nesta PoSIC.

Art. 32. A Estrutura de SIC deverá institucionalizar um modelo de GSIC para a EPL capaz de apoiar os diversos níveis hierárquicos da Empresa no objetivo de integrar os controles e processos de SIC aos processos organizacionais existentes.

Parágrafo único. A participação na referida estrutura e eventuais grupos de trabalho não enseja remuneração de qualquer espécie ou quaisquer criações de cargos além daqueles já existentes na estrutura regimental da EPL.

Art. 33. A Estrutura de Gestão de SIC é composta por:

I. Comitê de Segurança da Informação e Comunicações – CSIC;

II. Gestor de SIC; e

III. Equipe de Tratamento e Resposta a Incidentes de Rede – ETIR.

Parágrafo único. Os responsáveis por presidir ou coordenar as instâncias que formam a referida Estrutura de SIC deverão garantir, em consonância com suas atribuições específicas, o cumprimento do disposto no capítulo IV desta PoSIC e o efetivo desempenho das competências da respectiva instância.

Art.34. Os membros da Estrutura de GSIC devem receber regularmente capacitação especializada nas disciplinas relacionadas à SIC.

Parágrafo Único. A Estrutura de GSIC deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais da EPL e as consequências que riscos poderão trazer ao cumprimento dessas exigências.

Art. 35. As competências específicas do CSIC estão definidas em seu Regimento Interno.

Art. 36. Compete ao Gestor de SIC em seu âmbito de atuação especifico:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - promover e acompanhar a realização de estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

V - manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;

VI – propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do CSIC;

VII – outras competências das instancias responsáveis pela aplicação desta política, no âmbito da EPL serão definidas no Regimento Interno do CSIC

Parágrafo único – O gestor de SIC deverá ser formalmente designado pela autoridade competente e é o responsável pelas ações corporativas de segurança da informação no âmbito da EPL.

Art. 37. Compete a ETIR em seu âmbito de atuação especifico:

I – executar os processos de SIC;

II – fornecer subsídios visando à verificação de conformidade de SIC;

III – avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

IV – executar as atividades de tratamento e resposta a incidentes de segurança da informação junto a equipes envolvidas;

V – emitir alertas sobre vulnerabilidades e outras notificações relacionadas à SIC no âmbito da EPL;

VI – avaliar o uso de ferramentas de SIC;

VII – analisar ataques e intrusões na rede da EPL;

VIII – executar ações necessárias para tratar quebra de segurança da informação;

IX – agir proativamente, com o objetivo de evitar que ocorram incidentes de segurança da informação;

X – realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

XI – obter informações quantitativas acerca dos incidentes ocorridos;

XII – propor ao CSIC, o plano de investimento em SIC.

CAPÍTULO VII
DA RELAÇÃO COM TERCEIROS

Art. 38. Nos editais de licitação, nos contratos, contratos de gestão, convênios, acordos e instrumentos congêneres de cooperação técnica com entidades prestadoras de serviços para a EPL deverá constar clausula especifica sobre a obrigatoriedade de observância a esta Política, bem como deverá ser exigida, da entidade contratada, a assinatura de Termo de Responsabilidade.

CAPÍTULO VIII
DAS PENALIDADES

Art. 39. Ações que violem esta PoSIC ou que quebrem os controles de segurança da informação e comunicações serão passíveis de sansões civis, penais e administrativas, conforme a legislação e normas em vigor.

Art. 40. Em nenhuma hipótese será permitido o descumprimento desta Política e/ou de suas Normas pela alegação de desconhecimento das mesmas por parte do usuário.

Art. 41. O descumprimento das disposições constantes nessa Política e/ou nas Normas sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 42. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na legislação pertinente.

CAPÍTULO IX
DAS DISPOSIÇÕES GERAIS

Art. 43. A PoSIC e os documentos dela derivados deverão ser revisados sempre que mudanças significativas na estrutura a EPL ocorrerem ou quando alterações em normas e outras políticas forem aprovadas, ou ainda periodicamente, sempre que se fizer necessário, não excedendo o período máximo de dois anos.

Art. 44. A PoSIC e as normas e os procedimentos de SIC a ela associados deverão ser amplamente divulgadas.

Art. 45. O Gestor de SIC e a ETIR da EPL deverão ser designados em até 30 (trinta) dias após a publicação deste ato.

Art. 46. Os casos não previstos nesta PoSIC deverão ser reportados ao CSIC;

Art. 47. Esta Política Interna entrará em vigor a partir da data de sua publicação.

Art. 48. Fica revogada a Resolução nº 3, de 14, 07, 2015.