ENBPar
Empresa Brasileira de Participações em Energia Nuclear e Binacional

POLÍTICA DE SEGURANÇA **DA INFORMAÇÃO E COMUNICAÇÃO**

MINISTÉRIO DE MINAS E ENERGIA

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

EMPRESA BRASILEIRA DE PARTICIPAÇÕES EM ENERGIA NUCLEAR E BINACIONAL S.A.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ÍNDICE

GLOSSÁRIO

TIC – Tecnologia da Informação e Comunicação;

ATIC – Ativo de Tecnologia da Informação e Telecomunicação;

HOUSING-HOSTING – Ambiente seguro, confiável, redundante e flexível, que permite alojar a infraestrutura própria ou aquela proporcionada por prestadores de serviço;

CLOUD COMPUTING – tecnologia que usa a conectividade e a grande escala da Internet para hospedar os mais variados recursos, programas e informações;

CETITE – Comitê Estratégico de Tecnologia da Informação e Telecomunicações da ENBPar;

LGPD – Lei Geral de Proteção de Dados;

ISACA – Information Systems Audit and Control Association, que representa uma associação internacional de profissionais focados em governança de tecnologia da informação;

ITGI – Instituto de Governança em Tecnologia da Informação, é uma instituição global, independente e sem fins lucrativos, voltada para o desenvolvimento de conhecimento e adoção de práticas de uso de sistemas de informação globalmente aceitos;

COBIT – Control Objectives for Information and Related Technologies, é um framework criado pela ISACA para gerenciamento de Tecnologia da Informação (TI) e Governança de TI;

ABNT – Associação Brasileira de Normas Tecnicas, responsável pela publicação das NBRs;

ISO/IEC – Stands for the International Organization for Standardization e Stands for the International Electrotechnical Commission. Juntas, as duas organizações trabalham para manter e promover padrões nos campos da ciência e da tecnologia;

SI – Segurança da Informação;

SLA – Acordo de Niveis de Serviço;

CAPÍTULO I

OBJETO

Preservar a Segurança das Informações para apoiar na promoção da eficiência, eficácia e competitividade empresarial, de modo seguro, garantindo a sua confidencialidade, integridade, disponibilidade e legalidade, assim como dos Ativos de Tecnologia de Informação e Telecomunicação (ATICs) que as sustentam, de forma alinhada com o Planejamento Estratégico Empresarial.

Estabelecer por meio de sua Diretoria Executiva as orientações estratégicas de segurança aplicáveis quanto ao uso das Informações e dos ATICs da ENBPar, definindo os controles de segurança aplicáveis de acordo com os níveis dos riscos envolvidos.

CAPÍTULO II

CONCEITOS

- Ameaça
  Causa potencial de incidente indesejado que pode resultar em danos e perdas para uma organização.
- Ativo
  Qualquer recurso que tenha valor para uma organização.
- Ativos de Tecnologia de Informação e Telecomunicação (ATICs)
  Todo elemento que manuseia, processa ou guarda informações.
- Colaborador
  Funcionário e estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor, cliente, menor aprendiz, ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indiretamente, com a ENBPar.
- Evento de Segurança da Informação e Telecomunicação
  Ocorrência identificada de um estado de sistema, serviço ou rede, indicando possível violação à Política de Segurança da Informação e Telecomunicações ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- Internet
  Rede mundial de computadores, na qual o usuário pode, a partir de um computador, caso tenha acesso e autorização, obter informação de qualquer outro computador que também esteja conectado à rede.
- Risco
  Combinação da probabilidade de um evento e de suas consequências que podem causar danos a uma organização, perda de informações, perda financeira, parada de um serviço, dentre outros.

- Controle
  Processos internos específicos que têm o objetivo de fazer com que a empresa não seja prejudicada pelos riscos já conhecidos e que apresentam diferentes impactos e probabilidades de acontecer.
- Plano de TIC para Continuidade de Negócio
  Conjunto de estratégias e planos de ação preventivos que tem por objetivo garantir o pleno funcionamento dos serviços essenciais de uma empresa durante quaisquer tipos de falhas, até que a situação seja normalizada.
- Centro de Contingências de TIC
  Site de processamento alternativo com capacidade de assegurar a continuidade de negócios da empresa, por meio da recuperação dos serviços de TIC que possam eventualmente sofrer alguma interrupção importante, podendo assumir a modalidade de Housing-Hosting, Cloud Computing e/ou infraestrutura física (salas de usuários e escritórios), de acordo com as necessidades específicas de cada empresa.
- Violação
  Qualquer atividade que desrespeite as diretrizes estabelecidas na Política ou em quaisquer dos demais instrumentos regulamentares que as complementem.
- Gestor da Informação

  Colegiado, autoridade ou dirigente responsável por classificar as informações sob sua gestão e definir procedimentos e critérios de acesso.
- Custodiante da Informação

  Qualquer pessoa que detém a posse da informação, responsável por garantir a segurança da informação sob sua posse e comunicar sobre situações que comprometam essa garantia.
- Gestor de Unidade ou Subunidade

  Responsável por conscientizar seus colaboradores em relação aos conceitos e práticas de segurança da informação, bem como incorporá-las aos processos de trabalho da unidade. Em caso de comprometimento da segurança da informação, devem tomar medidas administrativas para que sejam adotadas ações corretivas em tempo hábil.
- Gerência Executiva de Segurança da Informação
  Área formal subordinada à Superintendência de Tecnologia da Informação e Telecomunicações, responsável pelo apoio às unidades da ENBPar na definição de procedimentos para proteção de suas informações, assim como monitorar e avaliar as práticas de segurança da informação e coordenar ações de conscientização e treinamento, bem como de tratamento de incidentes de segurança da informação.
- Comitê Estratégico de Tecnologia da Informação e Telecomunicações da ENBPar - CETITE
  Constituído por representantes das diversas áreas de negócio, o CETITE é responsável por formular e conduzir diretrizes, analisa a efetividade e propõe melhorias para a Política de Segurança Institucional.

CAPÍTULO III
REFERÊNCIAS

- Instrução Normativa IN 01/2008 GSI – Disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Disponível em: https://www.gov.br/governodigital/pt-br/legislacao/14_IN_01_gsidsic.pdf
- Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Diário Oficial da União. Brasília, DF, 13 de jun. 2000. p.2. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3505.htm
- Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5°, no inciso II do § 3° do art. 37 e no § 2° do art. 216 da Constituição Federal; altera a Lei n° 8.112, de 11 de dezembro de 1990; revoga a Lei n° 11.111, de 5 de maio de 2005, e dispositivos da Lei n° 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União. Brasília, DF, 18 de nov. 2011. p.1. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm
- Lei 13.709/2018 (LGPD) que tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Cria um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
- Norma Complementar nº 01/IN01/DSIC/GSIPR : Atividade de Normatização. Diário Oficial da União. Brasília, DF, 15 de out. 2008. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_1_normatizacao.pdf>.
- Norma Complementar nº 02/IN01/DSIC/GSIPR: Metodologia de Gestão de Segurança da Informação e Comunicações. Diário Oficial da União. Brasília, DF, 14 de out. 2008. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf>.
- Norma Complementar nº 03/IN01/DSIC/GSIPR: Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Diário Oficial da União. Brasília, DF, 03 de jul. 2009. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf>.
- Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo: Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Diário Oficial da União. Brasília, DF, 17 de ago. 2009. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>.
- Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo: Disciplina a criação de

Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Diário Oficial da União. Brasília, DF, 17 de ago. 2009. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf>.

- Norma Complementar nº 07/IN01/DSIC/GSIPR: Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Diário Oficial da União. Brasília, DF, 7 de maio 2010. Seção 1. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf>.
- Norma Complementar nº 08/IN01/DSIC/GSIPR: Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Diário Oficial da União. Brasília, DF, 24 de ago. 2010. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf>.
- Norma Complementar nº 09/IN01/DSIC/GSIPR: Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta. Diário Oficial da União. Brasília, DF, 22 de nov. 2010. Seção 1. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_9_criptografia.pdf>.
- ISACA. ITGI. COBIT 4.1: Control Objectives for Information and Related Technology. 2007.
- ABNT ISO GUIA 73:2009 – Gestão de Riscos.
- ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.
- ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação.
- Código de Ética e de Conduta da ENBPar.

CAPÍTULO IV

PRINCÍPIOS

- DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.
- INTEGRIDADE: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
- CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

- AUTENTICIDADE: propriedade que garante que a autoria e a origem da informação sejam sempre identificáveL.
- Preservar e proteger a informação gerada, adquirida, processada, transmitida e armazenada por qualquer ATIC de propriedade e/ou responsabilidade da ENBPar, dos diversos tipos de ameaça.
- Formalizar e consolidar os principais aspectos de estruturação e estabelecimento das Diretrizes de Segurança que compõem a Política Integrada de TIC.
- Prevenir e reduzir os impactos gerados por incidentes de segurança, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação da ENBPar.
- Estabelecer as diretrizes estratégicas e responsabilidades relativas às questões relacionadas a segurança da informação, possibilitando a criação de normas, procedimentos e instruções de trabalho de segurança.
- Assegurar que o Gestor de Segurança da Informação e Telecomunicação possa realizar o gerenciamento da estrutura de Segurança dos ATICs, para alcance dos objetivos estabelecidos, definindo, analisando e priorizando as ações necessárias.
- Estabelecer um Plano Anual de Capacitação voltado à manutenção das habilidades além do aperfeiçoamento dos colaboradores da ENBPar na gestão de tecnologia e segurança da informação.

CAPÍTULO V

DIRETRIZES

- Abrangência

  A Política de Segurança em Tecnologia da Informação e Telecomunicações deve ser aplicada a todos os colaboradores que venham a ter acesso ou utilizam, direta ou indiretamente, as informações e os ATICs da ENBPar.

- Publicidade

  Deve ser assegurado pela ENBPar que esta política e suas normas complementares estejam amplamente divulgadas aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com a organização e que, direta ou indiretamente são impactados.

- Interpretação

  Esta Política e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível. Ou seja, tudo que não estiver expressamente permitido só poderá ser realizado após prévia autorização, devendo ser levado em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

- Disponibilidade

  A ENBPar deve garantir que a informação e/ou recurso esteja oportunamente acessível sempre que necessário e mediante a devida autorização para seu acesso e/ou uso.

- Integridade

  A ENBPar deve garantir que a informação esteja correta, verdadeira e não esteja corrompida, nem tenha perdido suas características originais.

- Confidencialidade

  A ENBPar deve garantir que a informação, quando necessária, esteja acessível apenas a determinados indivíduos e/ou processos e seja devidamente protegida do conhecimento alheio.

- Legalidade

  A ENBPar deve garantir que a informação e/ou recurso atenda aos requisitos de conformidade com a legislação vigente, inclusive aos requisitos de:

  - ✓ Autenticidade

    Deve garantir que a informação é procedente e fidedigna, sendo a mesma, capaz de gerar evidências (não repudiáveis) da autoria da entidade atribuída como sua criadora, editora e/ou emissora; e

  - ✓ Temporalidade

    Deve garantir que a informação com valor comprobatório para fins auditorias, legais e judiciais seja preservada na forma e pelo prazo mínimo prescrito na regulamentação competente.

- Propriedade

  As informações geradas, acessadas, manuseadas, armazenadas ou descartadas por um colaborador no exercício de suas atividades, bem como os ATICs disponibilizados, são de propriedade e/ou direito de uso exclusivo da ENBPar e devem ser empregadas unicamente para fins profissionais, limitado às atribuições de cargo e/ou função desempenhadas pelo colaborador, que deve cumpri-las dentro do padrão de conduta ética estabelecida pela ENBPar e em observância a sua obrigação legal de sigilo profissional.

- Utilização dos Recursos

  A ENBPar deve assegurar que seus ATICs sejam utilizados apenas para fins profissionais, de modo lícito, ético e aprovado administrativamente.

- Mobilidade e Redes Sociais

  Os ATICs fornecidos pela ENBPar podem ser utilizados para atualização de seus colaboradores, bem como estimular a cooperação entre eles. Desse modo, qualquer uso de ATIC que permita maior mobilidade, bem como a participação em ambientes de relacionamento, como Redes Sociais, deve estar diretamente relacionado a uma justificativa do negócio, com motivo estritamente de trabalho, no âmbito das atribuições do colaborador e o mesmo responde diretamente por qualquer dano causado, por ação ou omissão, resultante

de sua postura e/ou comportamento, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

- Controle de Acesso

  A ENBPar deve controlar o acesso aos seus ATICs. Desse modo, a Organização deve garantir que cada colaborador possua uma credencial de uso individual, intransferível e de conhecimento exclusivo. A ENBPar deve ainda orientar seus colaboradores sobre a responsabilidade quanto ao uso e sigilo além de coibir o compartilhamento de credenciais, sob qualquer hipótese.

- Ciclo de vida da Informação

  A ENBPar deve prover ferramentas que permitam ao colaborador aplicar as melhores práticas de segurança, em conformidade legal, no ciclo de vida da informação, deste a sua criação, registro e classificação, acesso, manuseio, reprodução, transmissão, guarda e descarte.

- Classificação da Informação

  A ENBPar deve assegurar que seus colaboradores respeitem controles compatíveis com a classificação da informação, através da implementação de ferramentas e formalização de processos em instrumento específico. A ENBPar deve ainda orientar seus colaboradores que, em caso de dúvida, as informações serão rotuladas no mínimo como de uso interno, ou seja, não passível de revelação, publicação ou compartilhamento externo.

- Propriedade Intelectual

  A ENBPar é a detentora, também, de todos os direitos patrimoniais relativos às suas marcas e nomes comerciais e, portanto, deve proibir o uso não autorizado de suas logomarcas, identidade visual e quaisquer outros sinais distintivos, atuais e futuros, em qualquer forma ou mídia, inclusive a Internet.

- Sigilo

  A ENBPar deve orientar seus colaboradores para não revelar, publicar ou divulgar quaisquer informações de propriedade ou sob a responsabilidade da Organização sem prévia autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que tais informações estejam claramente classificadas como públicas.

- Terceirização ou Prestação de Serviços

  Todos os relacionamentos e contratações em que haja o compartilhamento de informações da ENBPar e/ou a concessão de qualquer tipo de acesso aos seus ambientes e ATICs, devem ser precedidos por Termos de Confidencialidade e cláusulas que tratem especificamente da Segurança da Informação e Telecomunicação. A ENBPar deve prover auditorias periódicas que visem certificar o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

- Análise dos ATICs

A ENBPar deve analisar, em intervalos regulares, seus processos e ATICs, assegurando que estes estejam devidamente inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

- Ambientes de ATIC

  Deve ser assegurado pela ENBPar que os ambientes dos sistemas e processos que suportam os ATICS sejam confiáveis, íntegros e disponíveis a quem deles necessite para execução de suas atividades profissionais.

- Segurança Física e do Ambiente

  A ENBPar deve estabelecer perímetros de segurança para proteger as áreas que contenham ATICs, bem como inserir controles e registros apropriados para assegurar o acesso somente aos colaboradores autorizados e ATICs homologados.

- Desenvolvimento de Sistemas

  Deve ser atestado pela ENBPar que o desenvolvimento interno e/ou externo de sistemas, assim como os sistemas e produtos adquiridos no mercado, sejam providos dos requisitos de segurança necessários para garantir informações confiáveis, íntegras e oportunas.

- Documentação

  A ENBPar deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvem ATICs.

- Monitoramento

  A ENBPar deve comunicar os seus colaboradores sobre o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, seus ATICs, além de seus ambientes, físicos e lógicos, para verificação da eficácia dos controles implantados, proteção de seu patrimônio e reputação, rastreando eventos críticos e evidenciando possíveis incidentes.

- Inspeção

  Sempre que se constate risco, a ENBPar pode inspecionar fisicamente quaisquer recursos tipificados como ATICs que porventura interajam com seus ambientes, lógicos ou físicos e/ou suas informações, incluindo os ATICs de propriedade de terceiros, quando autorizada a sua entrada nas instalações da ENBPar, independentemente da interação com seus ambientes e informações.

- Equipe de gestão de riscos de TIC da ENBPar

  Responsável pelo diagnóstico preventivo para decidir quais riscos de TIC são aceitáveis e quais necessitam de controles especiais, priorizando seu tratamento e evitando a ocorrência de incidentes. A equipe de gestão de riscos de TIC, subordinada à Superintendência de TIC, em conjunto com as unidades técnicas, realiza a análise de riscos de segurança da informação em processos de trabalho da ENBPar. O apetite a risco, a probabilidade e o impacto da materialização do risco direcionam a definição dos controles a serem adotados para sua mitigação.

- Equipe de Resposta a Incidentes de TIC

A ENBPar deve adotar medidas preventivas para diminuir os riscos de incidentes de segurança da informação com a criação e manutenção de uma Equipe de Resposta a Incidentes em Segurança da Informação, que pode ter composição fixa ou variável, e seja competente e preparada para dar resposta a incidentes e tratamento aos casos deste tipo. Essa equipe deverá registrar e tratar os incidentes em segurança da informação, visando a tomada de ações corretivas em tempo hábil, assim como ações no sentido de prevenir a da ocorrência desses eventos indesejados. Para atuar na gestão de incidentes de SI relacionados aos serviços e soluções de TI, conta com o apoio da Gerência Executiva de Segurança da Informação, subordinada à Superintendência de Tecnologia da Informação e Comunicação.

- Comunicação de Incidentes

  A ENBPar deve possuir um canal de comunicação junto aos seus colaboradores para reportar imediatamente os casos de incidentes de segurança da informação, podendo fazer de modo formal ou com uso do recurso de denúncia anônima.

- Continuidade do Negócio

  As diretrizes desta Política devem orientar os processos e planejamento estratégico da ENBPar na disponibilidade e continuidade das operações dos ATICs, visando mitigar os riscos de interrupção causados por incidentes de segurança, através da combinação de ações de prevenção e recuperação, mantendo os níveis de serviço acordados.

- Violações e Penalidades

  As violações de segurança da informação devem ser avaliadas e quando constatado um incidente, deve ser aplicado sanções administrativas cabíveis previstas em cláusulas contratuais, regimento de pessoal e outros documentos regulatórios da organização, além da legislação vigente, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

- Tentativa de Burla

  A mera tentativa de burla às diretrizes e controles estabelecidos pela ENBPar, quando constatada, deve ser tratada como uma violação.

- Conformidade

  A ENBPar deve possuir e manter um programa de revisão/atualização, no mínimo bienal, dessa política e dos demais instrumentos regulamentares subordinados a ela, visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente.

- Alterações

  Deve ser assegurado pela ENBPar que as alterações desta política e de suas normas complementares sejam devidamente comunicadas aos seus colaboradores. Todavia, deve ser esclarecido que é responsabilidade de cada colaborador a consulta esporádica e voluntária para identificar possíveis atualizações dos instrumentos.

- Capacitação

A ENBPar deve possuir um Plano Anual de Conscientização em Segurança da Informação visando à capacitação e disseminação a cultura de Segurança da Informação junto aos seus colaboradores em relação ao uso ético, seguro e legal das novas tecnologias e ferramentas de trabalho, bem como das informações e recursos disponibilizados.

- Controle de acesso à informação

  O acesso à informação deve ser franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação. Deve haver equilíbrio para que não haja restrição demais ou de menos. O acesso às informações que não sejam públicas deve ser restrito às pessoas que tenham necessidade de conhecê-las e devem se submeter a controles compatíveis com a classificação quanto à confidencialidade. Havendo necessidade de acesso a informações não públicas por pessoas com vínculo transitório com o TCU, é obrigatório o aceite de termo de sigilo e responsabilidade.

CAPÍTULO VI

RESPONSABILIDADES

- A Diretoria Executiva da ENBPar deve aprovar a Política de Segurança em Tecnologia da Informação e Telecomunicações.
- O CETITE deve analisar e avaliar as ocorrências de violações e demais eventos negativos relativos a Segurança da Informação e Telecomunicação na ENBPar, acionando a área responsável por TIC ou outras áreas impactadas/responsáveis quando necessário; promover, de forma eficaz a divulgação e a conscientização sobre segurança de informação e telecomunicação na Organização; analisar criticamente e de forma periódica esta Política e os demais instrumentos regulamentares relacionados à mesma, revisando e avaliando se o Sistema de Gestão da Segurança da Informação e Telecomunicação continua alinhado com os requisitos de negócio da ENBPar.
- A Área responsável por TIC na ENBPar deve atuar como coordenadora/gestora da implementação e manutenção desta Política.
- O Gestor responsável pela Segurança da Informação e Telecomunicação deve identificar e analisar os riscos de segurança ligados aos ATICs para avaliar a necessidade de melhorias nos controles existentes; propor instrumentos regulamentares complementares específicos para a proteção dos ATICs; Apoiar as áreas na definição de controles adequados de Segurança da Informação e Telecomunicação; atuar pró-ativamente em relação às ameaças e aos incidentes reportando-os ao CETITE; participar na contratação e definição de métricas de qualidade e temporalidade (SLAs) de quaisquer serviços relacionados à gestão e segurança dos ATICs.
- A Equipe de Resposta a Incidentes deve avaliar, monitorar e gerir os eventos de segurança da informação, sejam eles detectados ou notificados, com o formalização de procedimentos para assegurar respostas rápidas, efetivas e ordenadas, acionando a área responsável impactada/responsável quando necessário.

- Aos Chefes das Unidades Organizacionais cabe gerenciar o cumprimento desta Política por parte de seus colaboradores, mapear, implantar e testar os controles de Segurança da Informação e Telecomunicação específicos dos processos de seu departamento, especialmente daquelas atividades que não sejam dependentes de ATICs.
- Os Colaboradores devem cumprir esta política e os demais instrumentos regulamentares relacionados à mesma, através do uso de forma responsável, profissional, ética e legal os ATICs, respeitando os direitos e as permissões de uso concedidas pela ENBPar.

CAPÍTULO VII

DISPOSIÇÕES GERAIS

- O presente documento deve ser lido e considerado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes, adotados pela ENBPar. Além disso, esta política deve ser desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

- A presente Política de Segurança da Informação e Telecouminicações da ENBPar entra em vigor na data de sua aprovação pela Diretoria Executiva e será arquivada na sede da Companhia e disponibilizado em seu sítio eletrônico.