**SUMÁRIO**

## 1. FINALIDADE

Estabelecer diretrizes de modo a possibilitar o sistema de gerenciamento da segurança cibernética e da informação de acordo com os requisitos de negócios da Equatorial Energia S/A e das companhias direta e/ou indiretamente por ela controladas (“Grupo Equatorial”).

Definir conformidade com leis e regulamentações, estabelecer melhores práticas, normas e padrões para proteção da Informação, assegurar a disponibilidade dos serviços, atividades, processos e sistemas complexos, contribuir com a regular continuidade dos negócios do Grupo Equatorial.

Disseminar a cultura de segurança cibernética e da informação para reduzir eventuais riscos de incidentes cibernéticos e fortalecer a cultura organizacional.

## 2. CAMPO DE APLICAÇÃO

Esta Política de Segurança Cibernética e da Informação aplica-se aos ambientes de Tecnologia da Informação (TI) e Tecnologia Operacional (TO) de todas as empresas do Grupo Equatorial e, por conseguinte, a seus colaboradores próprios e empresas fornecedoras que possuam acesso às informações.

## 3. REPRESENTAÇÃO E RESPONSABILIDADES

### 3.1 Equatorial Energia S/A

- Ser a responsável e representar as companhias direta e/ou indiretamente controladas pela Equatorial Energia S/A, sendo elas as concessionárias de distribuição, transmissão e geração de energia elétrica, perante os órgãos reguladores quanto ao atendimento e cumprimento dos requisitos previstos nas regulamentações vigentes.
- Deve se comprometer na busca pela cooperação entre os diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos do setor, respeitadas as regras de confidencialidade das informações definidas pelo Agente.

### 3.2 Conselho de Administração

- Aprovar a Política de Segurança Cibernética e da Informação, através de ata de reunião, de acordo com o fluxo de homologação definido;
- Promover a cultura de segurança cibernética e da informação.

### 3.3 *Chief Executive Officer* - CEO

- Determinar o cumprimento da Política de Segurança Cibernética e da Informação, através de acompanhamento periódico e próximo às áreas de negócio responsáveis;
- Promover a cultura de segurança cibernética e da informação.

### 3.4 Comitê de Segurança Cibernética e da Informação

- Facilitar a implementação das políticas e procedimentos de segurança cibernética e da informação em todas as áreas e processos de negócio do Grupo Equatorial;
- Deliberar sobre assuntos sensíveis e desvios em relação a Política de Segurança Cibernética e da Informação.

### 3.5 Diretoria de Centro de Serviços Compartilhados

- Determinar o cumprimento da política de segurança cibernética e da informação;
- Garantir que a política de segurança cibernética e da informação seja cumprida, tratada com responsabilidade, zelo e transparência;
- Aprovar os recursos para investimentos para suportar o sistema de gestão de segurança cibernética da informação;
- Aprovar o tratamento dos riscos de segregação de função com o nível de risco alto;
- Apoiar as ações para promoção da cultura de segurança cibernética e da informação.

### 3.6 Superintendência de Telecomunicação e Informação (“Superintendência de TI Telecom”)

- Ser a responsável pela política de segurança cibernética e da informação perante os órgãos regulatórios e demais instituições;
- Aprovar as estratégias para contenção, mitigação e eliminação de crises decorrentes de incidentes críticos de segurança cibernética ou da informação que causem impacto ao negócio;
- Assegurar que objetivos da política de segurança cibernética e da informação estejam compatíveis com as diretrizes estratégicas do Grupo Equatorial;
- Estabelecer e coordenar o Comitê de Segurança Cibernética da Informação no Grupo Equatorial;
- Assegurar a melhoria contínua dos procedimentos de segurança cibernética e da informação, dentro do escopo de suas atribuições;
- Promover a cultura de segurança cibernética e da informação.

### 3.7 Superintendência Jurídica

- Garantir nas minutas dos contratos de prestação de serviços estejam contempladas as responsabilidades dos fornecedores quanto aos requisitos de segurança cibernética e da informação;
- Garantir, sob o aspecto jurídico, as ações requeridas durante crises em decorrência de incidentes cibernéticos críticos.

### 3.8 Gerência de Arquitetura e Segurança da Informação

- Definir estratégias para contenção, mitigação e eliminação de crises decorrentes de incidentes críticos de segurança cibernética ou da informação que causem impacto ao negócio;
- Estabelecer procedimentos técnicos e de gestão de incidentes cibernéticos;
- Estabelecer, manter atualizada e aplicar a política de segurança cibernética e da informação e demais normas vigentes e correlacionadas ao tema no sistema de gestão de documentos corporativos, para fins de homologação, armazenamento e consulta;
- Atuar como agente responsável pela governança desta política e pelas ações estratégicas e táticas sobre segurança cibernética e da informação, apoiando as áreas de negócio no momento da concepção de novos produtos e serviços;
- Realizar a avaliação de maturidade em segurança cibernética e da informação anualmente através de frameworks de mercado, com o objetivo de monitorar a aderência do ambiente tecnológico e de automação às melhores práticas;
- Manter-se atualizado em relação as tendências de mercado sobre segurança cibernética e da informação, novas tecnologias e adotar estratégias para implementá-las;
- Identificar e gerenciar riscos de segurança cibernética e da informação, em acordo com a metodologia utilizada pelo Grupo Equatorial;
- Promover, apoiar a cultura e orientar colaboradores próprios e fornecedores sobre o entendimento e a aplicabilidade das diretrizes de segurança cibernética e da informação;
- Propor orçamento e administrar projetos e iniciativas relacionadas ao gerenciamento da segurança cibernética e da informação;
- Estabelecer políticas, normas, procedimentos, melhoria contínua e/ou implementar tecnologias e serviços especializados, para todos os temas relacionados à segurança cibernética e da informação;

- Criar e gerir indicadores para monitoramento do ambiente de segurança cibernética e da informação;
- Estabelecer critérios técnicos de configuração segura para os ativos e sistemas de tecnologia;
- Proteger e manter atualizado os controles de segurança com as melhores práticas de mercado;
- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

### 3.9 Gerências de Sistemas

- Manter o inventário atualizado que contemple todos os ativos de tecnologia da informação, tecnologias da automação, sistemas corporativos, sistemas de técnicos e sistemas comerciais.

### 3.10 Gerência de Infraestrutura e Telecom

- Configurar os ativos de tecnologia da informação de TI e TO em conformidade com baseline de segurança cibernética;
- Implementar as regras e padrões de segurança definidos para a configuração dos ativos da rede de telecomunicações dos ambientes TI e TO;
- Atuar, conforme necessário, nos processos de gestão de incidentes cibernéticos para os ambientes TI e TO;
- Manter o inventário que contemple todos os ativos de tecnologia da informação, tecnologias da automação, sistemas corporativos, sistemas de automação e sistemas comerciais.

### 3.11 Gerência de Projetos e Soluções

- Garantir que os sistemas desenvolvidos ou adquiridos estejam de acordo com o baseline de sistemas de TI e TO e com as diretrizes de segurança cibernética e da informação.

### 3.12 Gerência de Compras e Contratação

- Solicitar e dar ciência aos potenciais fornecedores durante o processo de contratação quanto a necessidade de cumprirem todos os requisitos estabelecidos nos padrões de segurança cibernética e da informação, conforme o nível de complexidade do serviço que possuam acesso a informações críticas ou que manuseiam dados relevantes;
- Garantir que os padrões de segurança da informação estejam estabelecidos em todos os contratos de prestação de serviços.

**3.13 Gerência Corporativa de Governança, Compliance e LGPD**

- Atuar, de forma engajada e proativa para garantir a privacidade e proteção de dados em conjunto com a gerências de arquitetura e segurança da informação, direcionando os requisitos técnicos a serem seguidos;
- Realizar a revisão periódica e interpretação legal das diretrizes de segurança da informação e proteção de dados pessoais quanto ao atendimento de aspectos legais, recomendando melhorias, quando necessário.

**3.14 Gerência de Auditoria, Riscos e Controles Internos**

- Realizar a revisão periódica das diretrizes de segurança da informação, recomendando melhorias quando necessário;
- Realizar auditorias periódicas dos processos de segurança cibernética e da informação, de acordo com as diretrizes da política e melhores práticas de mercado;
- Apurar a divulgação, compartilhamento indevido de informações e os desvios de condutas dos colaboradores próprios e fornecedores na utilização dos recursos, reportando os resultados ao Comitê de Ética para que as medidas disciplinares sejam avaliadas;
- Definir a metodologia e executar a estratégia de gestão de riscos corporativos do Grupo Equatorial.

**3.15 Gerências de Gente e Gestão**

- Gerenciar o plano de desenvolvimento dos colaboradores próprios, através de treinamentos de segurança da informação oferecidos aos colaboradores próprios;
- Seguir o plano de conscientização em segurança cibernética e da informação com relação a colaboradores próprios e novos, para a disseminação da cultura de segurança cibernética;
- Conscientizar os novos colaboradores próprios sobre a importância em cumprir a política de segurança da informação, e assim contribuir para a disseminação da cultura de segurança cibernética;
- Aplicar as medidas disciplinares cabíveis, em conjunto com a Gerência do colaborador que deverá acontecer imediatamente após as apurações previstas na Política de Segurança Cibernética e da Informação.

**3.16 Gerência de Governança de Fornecedores**

- Conscientizar colaboradores dos fornecedores sobre a necessária observância à Política de Segurança Cibernética e da Informação;

- Gerir os acessos lógicos concedidos pelo Grupo Equatorial aos colaboradores dos fornecedores;
- Determinar e prover pessoas necessárias e competentes, para a implementação e manutenção do Sistema de Gestão de Segurança Cibernética e da Informação;
- Assegurar que os recursos tecnológicos, as informações e sistemas cedidos a fornecedores sejam utilizados apenas para as finalidades determinadas, explícitas e legítimas.

**3.17 Gerência de Seleção e Cultura Organizacional**

- Auxiliar na construção e manutenção do plano de comunicação da segurança cibernética e da informação;
- Promover campanhas que possam contribuir para formação da cultura da Segurança Cibernética e da Informação.

**3.18 Gerência de Regulação (Geração, Distribuição e Transmissão)**

- Garantir que a política de segurança cibernética e da informação e demais normas vigentes e correlacionadas existentes no sistema de gestão de documentos corporativos estejam aderentes à regulamentação vigente;
- Intermediar as interações entre a Agência Reguladora e o Grupo Equatorial de modo a atender as solicitações de informações, esclarecimentos, documentos e comprovantes de atendimento à regulamentação vigente e possíveis fiscalizações com apoio das áreas responsáveis.

**3.19 Gerência de *Facilities***

- Desenvolver e aplicar medidas de proteção física para assegurar que as instalações do Grupo Equatorial contra caso fortuito e força maior, a exemplo de desastres naturais.

**3.20 Executiva de Segurança Empresarial**

- Implantar medidas de segurança que possam proteger os perímetros das instalações;
- Garantir os controles de acesso físico às instalações do Grupo Equatorial.

**3.21 Liderança das Áreas de Negócio**

- Orientar os colaboradores sob sua gestão, para a adequada utilização dos recursos de tecnologia da informação;
- Gerir os acessos lógicos concedidos pelo Grupo Equatorial aos colaboradores dos fornecedores;

- Identificar riscos de segregação de funções críticas nos sistemas utilizados pelas áreas sob sua responsabilidade, e notificar o gerente de arquitetura e segurança da informação para que a segregação dos perfis de acesso possa ser implementada;
- Fiscalizar o cumprimento da política de segurança cibernética e da informação e normas vigentes e correlacionadas pelos colaboradores próprios e de fornecedores que estão sob sua gestão, relatando os desvios de condutas dos Colaboradores ao Canal Confidencial;
- Aplicar as medidas disciplinares recomendadas pelo Comitê de Ética aos seus colaboradores próprios;
- Gerir os contratos de seus fornecedores de forma a garantir o cumprimento da política de segurança cibernética e da informação e relatar qualquer desconformidade ao respectivo assessor legal.

**3.22 Todos os Colaboradores Próprios e de Fornecedores**

- Conhecer e cumprir as diretrizes estabelecidas na política de segurança cibernética e da informação e das normas vigentes e correlacionadas;
- Atuar de forma engajada e proativa em relação a segurança da informação, incluindo, mas não se limitando ao cumprimento das diretrizes da política de segurança cibernética e da informação;
- Zelar pela proteção da reputação, da imagem e do patrimônio do Grupo Equatorial, evitar a exposição desnecessária das informações, inclusive nas redes sociais, agir com responsabilidade no uso dos recursos;
- Assegurar que os recursos tecnológicos, as informações e os sistemas sejam utilizados apenas para as finalidades determinadas;
- Zelar pela segurança de sua identidade digital, devendo ser tratada de forma confidencial e exclusiva, não compartilhando, divulgando ou transferindo a terceiros;
- Comunicar ameaças digitais e possíveis incidentes cibernéticos por meio dos canais de comunicação disponíveis.

**3.23 Fornecedores**

- Cumprir todos os requisitos estabelecidos política de segurança cibernética e da informação e normas vigentes e correlacionadas.

## 4. DEFINIÇÕES

As definições dos termos técnicos apresentados nesta Política de Segurança Cibernética e da Informação e da Informação estão disponíveis no documento “GL. 00001.EQTL - Glossário de Termos Técnicos”.

## 5. REFERÊNCIAS

**Resolução Normativa ANEEL Nº 964, de 14 dezembro de 2021** – A Resolução Normativa ANEEL Nº 964 que dispõe sobre a Política de Segurança Cibernética e da Informação a ser adotada pelos agentes do setor de energia elétrica;

**Manual de Procedimentos da Operação ONS - Módulo 5 - Submódulo 5.13 - RO-CB.BR.01 –** O manual dispõe sobre os controles mínimos de segurança cibernética que devem ser adotados no Ambiente Regulado Cibernético que se conecta ao ONS;

**Lei 13.709, de 14 de agosto de 2018** – A Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, e o livre desenvolvimento da personalidade da pessoa natural.

**Norma ABNT NBR/ISO/IEC 27001:2022** – Sistemas de Gestão de Segurança da Informação e Comunicações – (Requisitos) – Que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações.

**Norma ABNT NBR/ISO/IEC 27002:2022** – Código de Prática para controles de Segurança da Informação – Que institui o código de melhores práticas para a Gestão de Segurança da Informação e Comunicações.

**Norma ABNT NBR/ISO/IEC 22301:2012** – Sistema de Gestão de Continuidade de Negócios – (Requisitos) – Que estabelece um fluxo de trabalho para planejar, implantar, operar, monitorar, revisar, e manter a melhoria contínua do Sistema de Gestão de Continuidade de Negócios;

**Norma ABNT NBR/ISO/IEC 27005:2019** – Gestão de Riscos de Segurança da Informação – Provê o fornecimento de diretrizes para o processo de gestão de riscos da segurança da informação.

## 6. ESTRUTURA NORMATIVA

GL.00001.EQTL. Glossário de Termos Técnicos;

MN.00008.EQTL. Cartilha PSI Política de Segurança da Informação;

MN.00020.EQTL Política de Segurança Cibernética e da Informação na Gestão com Fornecedores;

NP.00036.EQTL Classificação das informações;

NP.00049.EQTL Gestão de incidentes de Segurança Cibernética;

NP.00034.EQTL Conscientização e Treinamento em Segurança da Informação;

NP.00055.EQTL Gestão de Riscos de Segurança da Informação;

NP.00044.EQTL Gestão de Acesso Lógico;

NP.00190.EQTL Acesso Datacenter, Sala de Telecomunicação e Proteção dos Equipamentos de TI;

NP.00053.EQTL Acesso Remoto;

NP.00051.EQTL Penalidades de Segurança da Informação;

NP.00035.EQTL Gestão de Eventos e Monitoramento;

NP.00038.EQTL Gestão de Vulnerabilidades Técnicas;

NP.00192.EQTL Uso de Serviços de Rede;

NP.00193.EQTL. Gestão de Mudança de Sistema e dos Serviços de TI;

NP.00054.EQTL  Acesso Banco de dados;

NP.00037.EQTL  Acesso Identidades Privilegiadas;

NP.00041.EQTL Transferência da Informação;

NP.00042.EQTL  Política de Backup e Restore;

NP.00056.EQTL Gestão de Malware;

NP.00039.EQTL Controles Criptográficos;

NP.00043.EQTL Segurança em Nuvem;

NP.00040.EQTL Gestão de Disponibilidade;

NP.00221.EQTL Continuidade dos Serviços de TI;

NP.00050.EQTL Uso de Dispositivos Móveis;

NP.00048.EQTL Aquisição, Desenvolvimento e Manutenção de Sistemas;

NP.00045.EQTL Gestão de ativos de TI;

NP.00222.EQTL Uso de software;

NP.00008.EQTL. Política de Gestão de Riscos;

## 7. DIRETRIZES

Esta Política entrará em vigor na data da sua publicação e estará sujeita a revisões anuais, conforme item 10 Controle de Revisões desta Política de Segurança Cibernética e da Informação, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos do Grupo Equatorial.

### 7.1 Princípios desta Política

As ações relacionadas com a segurança da informação do Grupo Equatorial são norteadas pelos seguintes princípios:

- Confidencialidade: Garantia de que a informação somente estará disponível e revelada para o usuário previamente autorizado a acessá-la, em função de necessidade de seu exercício profissional contratado pelo Grupo Equatorial;
- Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que for utilizar um serviço, respeitando os acordos de nível de disponibilidade previamente acertados;
- Integridade: Garantia de que a informação não foi modificada, corrompida por aspectos de ambiente físico ou falhas no ambiente lógico ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino.

### 7.2 Acesso Lógico

As seguintes diretrizes devem ser consideradas para o acesso lógico à informação:

a) Os processos de gestão dos acessos lógicos do Grupo Equatorial devem ser conduzidos por um time responsável e especializado, que tratará de qualquer sistema, independentemente de ser interno ou em nuvem;
b) O acesso a qualquer sistema tecnológico deve ser protegido por credenciais de acesso, certificados, tokens, ou qualquer outro método seguro de identificação e autenticação;
c) O acesso às informações e sistemas do Grupo Equatorial devem ser permitidos somente após um processo formal de autorização composto por, no mínimo, um registro feito pelo Gestor do Colaborador solicitante ao time de gestão de acesso responsável;

d) As credenciais de acesso a sistemas e informações, compostas por usuário e senha, devem ser concedidas pelo Grupo Equatorial a colaboradores próprios e de fornecedores somente para o uso em atividades relacionadas a seu trabalho, pelo tempo em que perdurar seu vínculo com a empresa;

e) Os acessos dos colaboradores próprios e fornecedores devem ser desativados quando eles forem desligados ou tiverem seus contratos de prestação de serviços encerrados, conforme norma NP.00044.EQTL.Gestão de Acesso Lógico;

f) É proibido transferir, compartilhar, emprestar ou revelar a senha das credenciais de acesso, que foram concedidas pelo Grupo Equatorial a outros colaboradores ou outros fornecedores, devendo ser tratado de forma confidencial e exclusiva;

g) Todos os perfis de usuários para acesso às informações ou sistemas de média e alta criticidade devem ser revisados periodicamente pela equipe responsável de gestão de acesso, seguindo os critérios de segregação de função e observando o princípio de acesso mínimo e necessidade de conhecimento;

h) O acesso lógico aos ativos de tecnologia da informação, tecnologia da automação, sistemas de informação e/ou sistemas técnicos que suportam os processos de negócio do Grupo Equatorial deve ser identificado, controlados e protegidos.

i) Todos os colaboradores próprios e de fornecedores devem ser identificados individualmente por meio de uma credencial de acesso e senha.

j) Todas as credenciais de acesso devem seguir o princípio de minimização, ou seja, dar acesso ao mínimo necessário para que o colaborador exerça suas funções dentro do Grupo Equatorial;

k) Identidades de acesso genéricas ou de serviço nos ativos de tecnologia da informação, sistemas de informação e/ou sistemas técnicos que suportam os processos de negócio do Grupo Equatorial são permitidas exclusivamente para integrações e/ou conexões;

l) Não é permitido que identidades genéricas e de serviços sejam utilizadas por colaboradores próprios ou de fornecedores para fazer acesso a sistemas e/ou demais componentes de tecnologia ou automação. Qualquer exceção deve ser aprovada formalmente pela Gerência de Arquitetura e Segurança da Informação;

m) Deve ser estabelecido um processo formal para gestão das identidades privilegiadas concedidas a colaboradores próprios e fornecedores.

### 7.3 Análise de Vulnerabilidades Técnicas

As seguintes diretrizes devem ser consideradas para a análise de vulnerabilidades técnicas:

a) Deve ser estabelecido um processo de gestão de vulnerabilidades para cobrir todo e qualquer tipo de ativo de tecnologia da informação (TI) ou tecnologia da automação (TO);
b) Deve ser estabelecida e mantida uma listagem que contemple todos os equipamentos e sistemas críticos do Grupo Equatorial, ou seja, aqueles sistemas que mediante falha pode levar a perda econômica significativa, dano físico ou ameaça à vida humana;
c) Deve ser realizada análise de vulnerabilidades de forma automatizada e periódica através de softwares especializados, com o objetivo de identificar a necessidade de:
    - Instalação de patches de segurança;
    - Atualização, upgrade ou desinstalação de softwares; e,
    - Remoção de softwares maliciosos.

    A análise deve ser realizada nos sistemas técnicos e ativos de automação pelo menos semestralmente, e as vulnerabilidade corrigidas em até 180 dias;
d) Devem ser contempladas no Plano de Análise de Vulnerabilidades Técnicas, no mínimo, as simulações de cenários e ameaças para testes de resiliência, de análise das ferramentas e da capacidade e tempo de resposta;
e) Devem ser realizados testes de vulnerabilidades técnicas periodicamente nos equipamentos críticos que compõem a infraestrutura do Grupo Equatorial;
f) Deve ser garantida a capacidade para prevenção, detecção, resposta e redução de vulnerabilidade a incidentes cibernéticos do Grupo Equatorial;
g) Ativos que não suportem a análise automatizada devem realizar a análise de forma manual, através de checklist de segurança do ativo, incluindo, mas não se limitando a análise de CVEs disponíveis para:
    - Sistema operacional e patches de segurança;
    - Softwares e versões instaladas; e,
    - Serviços inseguros;
h) Nos casos em que não for possível eliminar totalmente o risco associado às vulnerabilidades de segurança da informação identificadas, devem ser estabelecidos termos de aceitação do risco, nos quais se registrem o motivo, os profissionais aprovadores e a validade do documento.

### 7.4 Aquisição, Desenvolvimento e Manutenção Segura de Sistemas de TI e TO

As seguintes diretrizes devem ser consideradas para aquisição, desenvolvimento e manutenção segura de sistemas de TI e TO:

a) Os sistemas de informação desenvolvidos ou adquiridos pelo Grupo Equatorial devem contar com atributos e funcionalidades de segurança que ofereçam proteção adequada;

b) Os requerimentos devem ser identificados e documentados na fase de concepção do sistema, para assegurar que as demandas de segurança sejam atendidas;

c) Devem ser estabelecidos controles que previnam erros de operação, perda ou vazamento de informações e de dados pessoais;

d) Todo sistema deve ser documentado, tornando sua implantação e operação independentes de conhecimentos informais;

e) Os sistemas devem ser protegidos contra alteração indevida, evitando a exposição de dados estratégicos e dados pessoais;

f) O acesso ao código fonte das aplicações deve ser adequadamente protegido;

g) Dados pessoais ou dados pessoais sensíveis reais não devem ser utilizados em ambientes de teste, homologação e aplicativos. Neste caso, os dados utilizados em ambientes não produtivos devem estar anonimizados;

h) Fornecedores e Colaboradores que desenvolvam sistemas para uso do Grupo Equatorial devem assinar termos de responsabilidade, e se submeterem a todas as políticas de segurança pertinentes;

i) O desenvolvimento de sistemas fora da Superintendência de TI e TELECOM para atendimento às necessidades operacionais de outras áreas deverá ser controlado e auditado previamente pela Gerência de Arquitetura e Segurança da Informação, sendo condição para sua efetivação;

j) O desenvolvimento de sistemas deve seguir as boas práticas de mercado referentes ao desenvolvimento seguro, bem como as diretrizes da Superintendência de TI e TELECOM sobre;

k) Todos os ativos de tecnologia devem ser devidamente homologados pela Superintendência de TI e TELECOM, sendo a referida homologação condição para regularidade;

l) Os ambientes de desenvolvimento, teste e produção devem ser segregados física ou logicamente, evitando o acúmulo de acessos de desenvolvedores ao ambiente de produção;

m) Devem ser estabelecidos requisitos de segurança necessários para a aquisição ou desenvolvimento de novos sistemas para qualquer ambiente, assim como as possíveis alterações e/ou atualizações em sistemas devem atender aos requisitos de segurança estabelecidos;

n) As aquisições de software e sistemas de TI e TO, assim como o desenvolvimento e manutenção de ativos tecnológicos, devem garantir a adoção e a manutenção dos requisitos previamente definidos nas *baselines*, padrões e normas de segurança cibernética definidas pelo Grupo Equatorial;
o) Deve-se estabelecer um processo de validação dos requisitos de segurança na análise crítica de novas soluções para TI e TO, assim como na análise crítica de soluções existentes que sofreram alterações significativas;
p) Os requisitos de segurança necessários para assegurar a confidencialidade, integridade, disponibilidade e conformidade de sistemas e dados do ambiente operacional devem ser garantidos;
q) Dados pessoais ou dados pessoais sensível reais não devem ser utilizados em ambientes de teste e homologação. Neste caso, os dados utilizados em ambientes não produtivos devem estar anonimizados.

### 7.5 Backup, Arquivamento e Restauração

As seguintes diretrizes devem ser consideradas para a backup, arquivamento e restauração:

a) Um plano de backup deve ser criado Superintendência de TI e TELECOM para atender os requisitos de retenção e guarda de dados do Grupo Equatorial, conforme os requisitos de negócio;
b) Os resultados dos *backups* devem ser periodicamente validados, com frequência adequada e possíveis falhas identificadas devem ser reportadas como incidentes;
c) O processo de restauração deve ser testado nos sistemas críticos de forma amostral, no mínimo, anualmente. Casos em que não for tecnicamente possível a sua execução devem ter controles compensatórios;
d) O tempo de vida do *backup* deve levar em consideração as necessidades do negócio e as exigências legais e regulatórias.

### 7.6 Classificação da Informação relacionadas aos ambientes de TI e TO

As seguintes diretrizes devem ser consideradas para a classificação da informação relacionadas aos ambientes de TI e TO:

a) Todas as informações do Grupo Equatorial devem ser atribuídas a um proprietário formalmente designado;
b) Todas as informações devem ser classificadas conforme a NP.00036.EQTL Classificação das informações, de acordo com seu valor, grau de sigilo, criticidade e sensibilidade perante o

negócio, de forma que sejam adotados os mecanismos de proteção adequados, balanceando custo e complexidade do controle;

c) Devem ser atribuídas às informações sem classificação explícita um grau de confidencialidade elevado, não sendo permitido o seu repasse ou divulgação para qualquer pessoa que não seja do Grupo Equatorial, exceto quando se tratar de informações públicas e de mercado devidamente autorizadas;

d) Todos os colaboradores devem tratar as informações do Grupo Equatorial de acordo com seu nível de classificação, de forma a protegê-las contra atos ou acessos indevidos, ou divulgação não autorizada.

### 7.7 Criação e manutenção do Comitê de Segurança da Informação

As seguintes diretrizes devem ser consideradas para criação e manutenção do comitê de Segurança da Informação:

a) Deve ser garantida a existência de um Comitê de Segurança da Informação, composto por pessoal qualificado, ao qual devem ser concedidos poderes de decisão nas questões relativas ao seu propósito;

b) O Comitê de Segurança da Informação deve facilitar a implementação das políticas e procedimentos de segurança da informação, de modo a garantir que todos os riscos identificados sejam gerenciados de acordo com os parâmetros estabelecidos pelo Grupo Equatorial;

c) O acionamento do Comitê de Segurança da Informação deverá ser realizado por um responsável da área de segurança da informação formalmente definido pelo Grupo Equatorial. O canal de acionamento de seus integrantes deve ser garantido, ágil e eficiente;

d) A composição do Comitê de Segurança da Informação deve ser suficientemente abrangente e multidisciplinar, e definida em ata de reunião da Alta Administração.

### 7.8 Comportamento Seguro

As seguintes diretrizes devem ser consideradas para o comportamento seguro:

a) Os ativos tecnológicos, serviços de tecnologia e todos os sistemas da organização de propriedade ou custódia do Grupo Equatorial devem ser utilizados de acordo com os interesses do Grupo e para a prestação dos seus serviços, atendendo aos requisitos e respeitando as regras;

b) Todo colaborador próprio ou de fornecedores que se distanciar do recurso de tecnologia da informação de propriedade do Grupo Equatorial que estiver em sua posse ou uso, especialmente a sua estação de trabalho e o dispositivo móvel, deverá realizar o processo de bloqueio;

c) Cada colaborador deve assumir um comportamento seguro e proativo, independente dos meios onde a informação que ele acessa esteja armazenada, ou pelo qual ela seja transmitida, impedindo seu vazamento para pessoas ou meios externos do Grupo Equatorial;
d) Os controles de segurança cibernética e da informação devem ser compatíveis com a relevância da instalação no contexto do SIN (SIN - Sistema Interligado Nacional), bem como, com a natureza e a complexidade dos serviços, atividades, processos e sistemas;
e) Os colaboradores próprios devem ser responsáveis por manter as informações do Grupo Equatorial em locais seguros. Isso se aplica às informações impressas, escritas em quadros ou em outras mídias físicas, que não devem ser deixadas desprotegidas em salas de reuniões, mesas ou qualquer local dentro ou fora da empresa;
f) O uso de recursos tecnológicos para gravação, fotografia e filmagem de qualquer reunião ou evento corporativo não é permitido sem prévia autorização e consentimento de todos os participantes;
g) O descarte de informações restritas ou confidenciais, contidas em qualquer meio, quer seja impresso, eletrônico, magnético, ou sob qualquer outra forma, deve ser feito de forma segura, garantindo a destruição dos dados de uma maneira que não possibilite sua recuperação.

### 7.9 Conformidade relacionadas aos ambientes de TI e TO

As seguintes diretrizes devem ser consideradas para a conformidade relacionadas aos ambientes de TI e TO:

a) O cumprimento e as aderência às leis, regulamentações, políticas, normas, obrigações contratuais, e demais padrões relacionados à segurança da informação, devem ser garantidos por todos os colaboradores do Grupo Equatorial;
b) Os responsáveis pelos recursos críticos do Grupo Equatorial devem garantir a retenção de evidências da execução de seus controles, para fornecimento em casos de auditorias ou necessidade de atendimento a regulamentações;
c) A versão atualizada da política de segurança cibernética e da informação e da informação deve ser publicada no sistema de gestão dos instrumentos normativos do Grupo Equatorial, e deverá ser de conhecimento de todos os seus colaboradores próprios e fornecedores.

### 7.10 Conscientização e Divulgação da Política de Segurança Cibernética e da Informação

As seguintes diretrizes devem ser consideradas para a conscientização e divulgação da política de segurança cibernética e da informação:

a) Esta política de segurança cibernética e da informação, e as demais normas vigentes e correlacionadas e demais padrões de segurança devem ser amplamente divulgados no processo de admissão e integração de novos colaboradores;
b) O programa de conscientização deve considerar controles de capacitação e de avaliação periódica de pessoal; plano de ação com medidas para a conscientização e educação de seus usuários sobre aspectos de segurança cibernética; e o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;
c) Programas de conscientização, divulgação e reciclagem do conhecimento desta política, bem como do conhecimento das demais normas e padrões de segurança relacionados, devem ser estabelecidos e praticados regularmente para garantir que todos os colaboradores e terceiros conheçam as diretrizes e suas responsabilidades relacionadas ao tema;
d) A divulgação dos objetivos, princípios e diretrizes de Segurança da Informação aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, programas de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança dentro do Grupo Equatorial;
e) A releitura desta política de segurança cibernética e da informação e normas vigentes e correlacionadas, mesmo que não seja diretamente solicitada, deve ser feita para melhor entendimento;
f) Capacitações e exercícios cibernéticos de segurança cibernética voltados para o ambiente de TI e TO devem ser conduzidos periodicamente para todos os colaboradores que atuam nestes ambientes.

### 7.11 Continuidade de Negócio, Recuperação de Desastre e Crise Cibernética

As seguintes diretrizes devem ser consideradas para continuidade de negócio, recuperação de desastre e crise cibernética:

a) Devem ser mantidos planos específicos de gerenciamento de crise e planos de recuperação que atendam aos ambientes de TI e TO do Grupo Equatorial, esses deverão ser, no mínimo, anualmente testados para garantir a continuidade operacional das atividades críticas, através da recuperação e restauração das operações, em caso de catástrofe, desastres ou interrupção dos serviços e processos críticos de TI e TO;
b) Deve-se garantir que todas as recomendações identificadas nos resultados dos testes/simulações sejam avaliadas, priorizadas e implantadas. E quando se tratar melhorias de processos, que os mesmos sejam padronizados;

c) Deve-se formalizar com as áreas de negócio a priorização de recuperação dos ambientes de TI e TO, tomando como base o plano de continuidade de negócios feitos pelas áreas de negócio do Grupo Equatorial;
d) Recomenda-se a criação de *playbooks* para os cenários críticos de indisponibilidade dos ambientes de TI e TO;
e) Deve-se estabelecer procedimentos de comunicação de crise (viés de crise cibernética).

**7.12 Proteção de Dados Pessoais e Informações Sensíveis**

As seguintes diretrizes devem ser consideradas para proteção de dados pessoais e informações sensíveis:

a) Todas as informações e dados pessoais de clientes, colaboradores próprios, fornecedores, entre outros, que venham a ser armazenadas, processadas ou colocadas sob custódia em ativos de tecnologia da informação ou operacionais do Grupo Equatorial, devem ser adequadamente protegidas;
b) Devem ser utilizados controles que visem proteger as informações, conforme os requerimentos de sua classificação;
c) Informações confidenciais do Grupo Equatorial não podem ser transportadas em qualquer meio sem as devidas autorizações e cautela;
d) As áreas de negócio devem sempre utilizar canais de comunicação seguros para o envio e recebimento de informações confidenciais entre fornecedores. Quando não for possível utilizar tais canais, deve-se fazer uso de controles ou senha forte para evitar eventuais vazamentos de informação.

**7.13 Privacidade**

A privacidade das informações sob responsabilidade do Grupo Equatorial deve ser assegurada através de políticas e controles, conforme previsto em leis e regulamentos pertinentes;

**7.14 Segurança de Fornecedores**

As seguintes diretrizes devem ser consideradas para a segurança de fornecedores:

a) Aquisições referentes a TI e TO, assim como desenvolvimentos, contratações e manutenções na área, devem ser gerenciadas pela Superintendência de TI e Telecom, de acordo com suas responsabilidades;
b) Toda aquisição de produtos ou serviços de tecnologia da informação, assim como pelo desenvolvimento e manutenção de ativos tecnológicos, devem:

- Garantir a adoção e a manutenção dos requisitos previamente definidos nas *baselines*, nos padrões e nas normas de segurança da informação;
- Validar os requisitos de segurança da informação na análise crítica de novas soluções, assim como na análise crítica de soluções antigas que sofreram alterações significativas; e,
- Garantir o atendimento aos requisitos de segurança necessários para assegurar a confidencialidade, integridade, disponibilidade e conformidade de sistemas e informações;

c) Os recursos de tecnologia da informação utilizados pelo Grupo Equatorial devem ser inventariados por responsáveis pela gestão de ativos de tecnologia da informação dentro da Companhia, de acordo com as boas práticas de segurança da informação;

d) Na contratação de serviços, os contratos firmados entre as partes devem conter cláusulas de confidencialidade. Outras cláusulas específicas de segurança da informação podem ser requeridas de acordo com o contexto do serviço contratado;

e) O sigilo necessário para as informações do Grupo Equatorial deve estar previsto em contrato e perdurar mesmo após o encerramento da prestação de serviços;

f) Fornecedores devem manter metodologias, procedimentos de gestão de incidentes e demais controles apropriados de segurança cibernética e da informação compatíveis com os controles estabelecidos pelo do Grupo Equatorial;

g) A veracidade das informações contidas em contratos deve ser adequadamente verificada;

h) Fornecedores que possuem acesso às informações do Grupo Equatorial e/ou estão conectados diretamente ou através de VPN ao ambiente de TI e TO devem obrigatoriamente seguir os padrões de segurança cibernética e da informação;

i) Adotar em suas infraestruturas controles e níveis de maturidade similares aos adotados pelo Grupo Equatorial enquanto contratante, e/ou, minimamente, atenderem às exigências legais e regulamentadoras, considerando escopo de suas atividades.

**7.15 Gestão de Incidentes de Segurança da Informação e Cibernética**

As seguintes diretrizes devem ser consideradas para a gestão de incidentes de segurança da informação:

a) Devem ser desenvolvidos mecanismos de detecção de incidentes cibernéticos no ambiente de TI e TO;

b) Devem ser considerados incidentes de segurança cibernética e/ou da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao

comprometimento de um ou mais dos princípios básicos de segurança da informação (confidencialidade, integridade, disponibilidade e conformidade), colocando o negócio em risco;

c) Violações ou tentativas de violação desta política, e de outras normas ou controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança;

d) Colaboradores próprios devem informar sobre todas as violações a esta política de que tomarem conhecimento, procurando imediatamente a equipe responsável por manter a segurança da informação no Grupo Equatorial;

e) A identificação de incidentes de segurança pode ocasionar o bloqueio imediato dos acessos dos colaboradores envolvidos, até que sejam concluídas as investigações necessárias;

f) Qualquer evento relacionado a ataques à segurança de um sistema, confirmados ou sob suspeita, deve ser resolvido de acordo com os procedimentos de resposta a incidentes de segurança cibernética;

g) Os procedimentos de resposta a incidentes de segurança da informação devem descrever as etapas de gestão do incidente, sua investigação e o recolhimento de provas e devem também:

- Permitir a detecção o mais rapidamente possível, e prover a capacidade de responder com a máxima eficácia, visando limitar os danos causados pelo incidente;
- Limitar as zonas de vulnerabilidade através da remediação de anomalias identificadas nos sistemas potencialmente afetados;
- Reter informações relevantes para investigações posteriores, e coleta de provas;
- Compilar um registro de incidentes de segurança, e prover estatísticas para uso na previsão de possíveis incidentes futuros;
- Identificar pontos de contato apropriados para o nível de severidade do ataque; e,
- Quando um incidente originado por ação mal-intencionada for encerrado, deve ser feita uma análise para identificar a origem do ataque e iniciar os procedimentos técnicos, administrativos ou judiciais apropriados.

h) Devem ser formalizados, os papéis e responsabilidades relacionados a gestão de incidentes de segurança cibernética para o ambiente de TI e TO;

i) Todos os incidentes referentes à vazamento de dados pessoais deverá ser imediatamente comunicados através do Portal de Serviços e ao Encarregado de dados, conforme previsto na política interna de proteção de dados pessoais;

j) Devem ser garantidos mecanismos para prevenir, mitigar e recuperar incidentes cibernéticos nas redes de informação e instalações, de modo a impedir que os incidentes afetem a operação da Companhia;

k) Devem ser mantidos registros de análise da causa raiz e do impacto operacional e do negócio em casos de incidentes de maior impacto para as atividades do Grupo Equatorial, abrangendo informações recebidas por fornecedores.

**7.16 Gestão de Riscos de Segurança Cibernética e da Informação**

As seguintes diretrizes devem ser consideradas para a gestão de riscos de segurança da informação:

a) Deve ser implementado e mantido um processo de gestão de riscos de segurança cibernética estruturado que contemple a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoramento dos riscos e vulnerabilidades aplicáveis ao ambiente de TI e TO que podem afetar negativamente as áreas e sistemas que suportam as operações e negócios do Grupo Equatorial;

b) Deve ser implementado e mantido um modelo de avaliação de maturidade de segurança cibernética, compatível com a estrutura do Grupo Equatorial, seu segmento e boas práticas de mercado, com aplicação de periodicidade minimamente anual;

c) O processo de gestão de riscos deve contemplar todos os ativos, sistemas e processos, quer sejam eles internos, em nuvem, ou conduzidos por fornecedores.

**7.17 Monitoramento de Segurança Cibernética e da Informação**

As seguintes diretrizes devem ser consideradas para o monitoramento de segurança da informação:

a) Todas as ações de colaboradores próprios, fornecedores e visitantes, realizadas remotamente ou nas dependências do Grupo Equatorial, abrangendo o acesso físico e/ou a utilização de recursos de tecnologia da informação e comunicação, devem ser passíveis de monitoramento, conforme leis e regulamentos estabelecidos;

b) As áreas de tecnologia da informação devem garantir a privacidade dos registros oriundos do monitoramento de acessos, e do uso de sistemas e serviços de tecnologia da informação;

c) Os registros obtidos através de monitoramento poderão ser utilizados em processos de investigação de incidentes e suspeitas de violação de leis e normas, assim como em processos judiciais e trabalhistas, a critério do Grupo Equatorial;

d) O Grupo Equatorial deve monitorar e supervisionar todos os ambientes físicos e lógicos de sua propriedade ou sob seu controle, sem haver a necessidade de prévio consentimento ou de

notificação de seus colaboradores próprios ou de fornecedores, podendo manter os registros do produto do monitoramento, sejam as informações ou dados que passarem por seus recursos de Tecnologia da Informação obtidos em suas instalações físicas;

e) Deve ser garantida a rastreabilidade das ações em sistemas que manipulem informações críticas;

f) Devem ser implementados para os ativos críticos do ambiente, mecanismos para inclusão das trilhas de auditoria (*logs)* geradas em um sistema de gerenciamento de eventos de segurança, juntamente com um processo para a realização de revisões periódicas das trilhas geradas.

**7.18 Registros de Auditoria**

As seguintes diretrizes devem ser consideradas para os registros de auditoria:

a) Todo evento de segurança da informação e todas as ações de usuários em sistemas críticos operacionais e de tecnologia da informação, sempre que possível, devem estar configurados para gerar trilhas de auditoria (*logs*), que deverão ser mantidas por um período mínimo adequado, em local centralizado e protegido contra acessos não autorizados;

b) Não deve haver nenhuma modificação na integridade das trilhas de auditoria (*logs*). Para tanto, não deve haver usuários com permissão para alterá-las;

c) Todos os acessos para consulta, cópia, tentativa de modificação ou de exclusão das trilhas de auditoria (*logs*) devem ser registrados;

d) Todas as falhas nos registros das trilhas de auditoria (*logs*) devem ser registradas, analisadas e respondidas com providências para correção imediata.

**7.19 Prevenção e Detecção de Intrusão**

As seguintes diretrizes devem ser consideradas para a prevenção e detecção de intrusão:

a) Para a prevenção e detecção de intrusão no ambiente de TI e TO, os recursos e sistemas críticos expostos na internet devem ser acompanhados e protegidos por sistemas de proteção como firewalls, soluções IDS/IPS e software *antimalware*;

b) Para os sistemas e ativos do ambiente que não suportarem o uso de credenciais e/ou credenciais únicas, pessoais e intrasferíveis, devem ser implementados controles compensatórios de segurança;

c) Sempre que as soluções detectarem ou responderem uma tentativa externa mal-intencionada, grave o suficiente para ameaçar os recursos do sistema de informação protegido, devem ser iniciados tanto uma análise estruturada quanto um procedimento de resposta.

### 7.20 Proteção contra Códigos Maliciosos nos ambientes de TI e TO

As seguintes diretrizes devem ser consideradas para a proteção contra códigos maliciosos nos ambientes de TI e TO:

a) Devem ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de *software* (tanto de usuário final como de servidores), visando prevenção, detecção, correção e erradicação de códigos executáveis maliciosos;
b) As ferramentas de proteção baseadas em assinaturas devem estar sempre atualizadas com suas últimas versões.
c) Devem ser implementados, sempre que possível, software *antimalware,* solução *IDS* para a proteção dos equipamentos que executem softwares nos ambientes, visando prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.

### 7.21 Segurança em Redes

As seguintes diretrizes devem ser consideradas para a segurança de redes:

a) Deve-se buscar a utilização segura das redes, dos sistemas que compõem os serviços de energia elétrica do Grupo Equatorial;
b) É necessário que existam controles tecnológicos para proteger o acesso entre redes (incluindo internet, redes públicas, extranets, acesso remoto, *wireless* e as diferentes redes de usuários);
c) Equipamentos com diferentes requerimentos de segurança devem ser segregados em redes diferentes;
d) Além do controle de acesso entre redes, a informação em trânsito também deve ser protegida, seguindo os requerimentos de classificação da informação;
e) O acesso remoto é permitido somente para situações em que ele seja indispensável. Este tipo de acesso deve ser documentado e protegido adequadamente, fazendo uso de, pelo menos, mecanismos de autenticação de dois fatores;
f) Os níveis de segurança esperados dos serviços de comunicações, que consideram fatores de confidencialidade, integridade e disponibilidade, devem ser estabelecidos nos contratos firmados com seus respectivos fornecedores;
g) Devem ser estabelecidos controles criptográficos para garantir os níveis de confidencialidade das informações trafegadas, considerando suas classificações;

h) Os sistemas de informação devem ser mantidos atualizados, seguindo o fluxo de gestão de mudanças estabelecido pelo Grupo Equatorial, para mitigar o risco de ameaças conhecidas;

i) Todos os recursos de Tecnologia da Informação de propriedade do Grupo Equatorial ou que necessitem estarem conectados à rede corporativa deverão possuir *software* antivírus, *firewall* para a proteção das redes mais críticas e *antimalware* homologado pela Gerência de Arquitetura e Segurança da Informação;

j) Devem ser consideradas para a segurança de redes no ambiente operacional:
   - Os ambientes corporativo e operacional logicamente segregados e suas interações asseguradas através de uma rede de perímetro (DMZ);
   - Os ambientes operacionais não diretamente expostos à Internet;
   - Controles implementados de portas de comunicação dos equipamentos que compõem a rede, desabilitando, por padrão, as portas de comunicação que não estiverem sendo utilizadas; e
   - Garantir ambientes de redundância para a infraestrutura de *data centers* dos ambientes operacionais.

**7.22 Segurança Física dos ativos TI e TO**

As seguintes diretrizes devem ser consideradas para a segurança física dos ativos de TI e TO:

a) Os equipamentos, instalações de processamento de informações críticas ou sensíveis e ativos dos ambientes de TI e TO devem ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais;

b) As salas destinadas aos equipamentos e ativos de infraestrutura, painéis de controle, comunicação e cabeamento deve possuir acesso autorizado, restrito, monitorado e controlado.

c) Os centros de controle e ambientes operacionais críticos devem permanecer sempre fechados e possuírem controles de acesso e monitoramento de segurança.

**7.23 Serviço em Nuvem**

As seguintes diretrizes devem ser consideradas para os serviços em nuvem:

a) A utilização de soluções de hospedagem externa, conhecidas como computação em nuvem, deve ser feita apenas pela equipe de TI, com embasamento em análise de risco, que levará em consideração a sensibilidade dos dados e processos em questão. Os serviços em nuvem devem:
   - Fazer uso de canais de tráfego de dados resguardados por protocolos seguros;
   - Fazer uso de sistemas de autenticação segura; e,

- Fazer segregações do ambiente, sem compartilhar estruturas lógicas com outros clientes.

b) Os acessos devem ser controlados por meio de *login* e senhas individuais, previamente fornecidos de acordo com a atividade de cada colaborador próprio, fornecedor ou administrador. Tanto seus acessos quanto suas ações devem ter registros em trilhas de auditorias.

**7.24 Utilização de Recursos de Tecnologia da Informação**

As seguintes diretrizes devem ser consideradas para a utilização de recursos de tecnologia da informação:

a) A utilização de qualquer recurso de tecnologia da informação deve ser, primeiramente, autorizada pelo gestor do colaborador, fornecedor ou pelo proprietário da informação, recurso ou sistema e a liberação deve ser concedida pela equipe de TI;
b) Os recursos de tecnologia da informação devem ser mapeados e mantidos atualizados;
c) Não é permitido que colaboradores próprios e de fornecedores realizem a instalação de qualquer *software* ou alteração de parâmetros de configuração em computadores do Grupo Equatorial. Tais operações devem ser realizadas por equipes de tecnologia da informação autorizadas, após processos de homologação e obtenção do licenciamento adequado. Softwares instalados indevidamente poderão ser automaticamente excluídos, sem prévio aviso;
d) A liberação de uso de celulares, *smartphones*, *tablets* e qualquer outro dispositivo do Grupo Equatorial deve ser permitido apenas após o atendimento integral dos requisitos de segurança definidos nas normas para esta categoria de dispositivos;
e) Documentos eletrônicos devem ser armazenados em repositórios centralizados de rede (servidores de arquivos) e/ou em nuvem do Grupo Equatorial, com as devidas proteções de segurança, como controle de acesso e *backup*;
f) Os sistemas, as informações e os serviços do Grupo Equatorial utilizados pelos colaboradores, no exercício de suas atividades, são de exclusiva propriedade do Grupo Equatorial, não podendo ser interpretados como de uso pessoal;
g) Fica vedada a utilização de equipamentos pessoais por colaboradores próprios ou de fornecedores, assim como os equipamentos de propriedade do Grupo Equatorial para as atividades não relacionadas ao uso de sua função.

**7.25 Registro das Evidências do Programa de Segurança Cibernética**

O Grupo Equatorial deve adotar um local para elaboração, registro e armazenamento seguro das evidências geradas no Programa de Segurança Cibernética, mantendo disponíveis as informações para os casos de auditorias internas, externas e comunicações necessárias com os órgãos reguladores.

O Grupo Equatorial deve manter registros e enviar para o órgão regulatório ou para a equipe de coordenação setorial designada as seguintes informações sempre que solicitadas:

- Os resultados dos modelos de maturidade aplicados em formato a ser definido;
- Os riscos cibernéticos identificados, com a respectiva forma de tratamento e os dados das equipes de prevenção; e
- Tratamento e resposta a incidentes cibernéticos.

## 8. CANAIS DE COMUNICAÇÕES E COOPERAÇÃO

O Grupo Equatorial deve adotar procedimento de compartilhamento de informações sobre ameaças e outras informações relativas à segurança cibernética de forma sigilosa e não discriminatória, sendo facultado o anonimato.

O compartilhamento de informações não pode ser restrito às empresas do mesmo grupo societário, respeitadas as informações classificadas pelo Grupo Equatorial como críticas ou que possam comprometer a sua própria segurança.

### 8.1 Canal Confidencial

Atitude suspeita ou desvio de conduta que coloque a Segurança da Informação em risco, deve ser informado imediatamente por meio do Canal Confidencial do Grupo através do endereço: https://www.canalconfidencial.com.br/equatorial/ ou via telefone no número 0800-300-4580.

### 8.2 Canal de Comunicação com Encarregado de Proteção de Dados Pessoais

Em caso de vazamentos de dados pessoais ou qualquer outra frente relacionada ao exercício de direitos dos titulares, regulados pela Lei n° 13.709/2018 – LGPD, deverá ser comunicado imediatamente no canal encarregado_lgpd@equatorialenergia.com.br.

### 8.3 Canal de Privacidade de Segurança

Uma vez que o evento de segurança cibernético é detectado, seja pelos usuários, empresas terceiras ou sensores de monitoramento, ele é reportado a Gerência de Arquitetura e Segurança através do Portal de Serviços na categoria privacidade e segurança, ou quando não for possível, para o e-mail infosec@equatorialenergia.com.br.

### 8.4 Canal de Comunicação com demais Órgãos Externos

O Grupo Equatorial deve notificar a equipe de coordenação setorial do órgão Regulatório designada dos incidentes cibernéticos de maior impacto que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários ou de dados.

- Que a notificação do incidente cibernético de maior impacto deve incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso;
- A notificação do incidente cibernético de maior impacto não exclui o atendimento de outras obrigações de comunicação previstas em leis, normas e regulamentos;
- A notificação deve ser realizada assim que o agente tiver ciência do incidente e de sua dimensão;

**Nota 1: A comunicação com demais órgãos externos, sobre assuntos relacionados a incidentes de segurança cibernética e da informação deve ser prevista e realizada pela Diretoria de Centro de Serviços Compartilhados, quando cabível, e com o suporte da Gerência de Comunicação Externa, *Marketing* e Sustentabilidade quando cabível, em caso de instauração de situação de crise.**

## 9. MEDIDAS DISCIPLINARES

O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança Cibernética e da Informação e da Informação e Normas vigentes e correlacionadas poderá resultar na aplicação das sanções previstas na Norma de Procedimento NP.00051.EQTL Penalidades de Segurança da Informação e legislação em vigor. O colaborador próprio ou fornecedor responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar ao Grupo Equatorial, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

## 10. CONTROLE DE REVISÕES

| REV | DATA (Elaboração/Revisão) | ITEM | DESCRIÇÃO DA MODIFICAÇÃO | RESPONSÁVEL |
|---|---|---|---|---|
| 00 | 17/06/2022 | Todos | Emissão Inicial | Humberto Luiz Queiros Nogueira |
| 01 | 25/10/2023 | Todos | Revisão geral para expandir a aplicabilidade desta política aos ambientes de tecnologia operacional | Tiago Barroso Oliveira |

O Fluxo de aprovação da criação e revisão desta Política de Segurança Cibernética e da Informação apresenta as seguintes fases:

**Tabela 2**: Fluxo de Aprovação

| **FASE** | **Atividade** | **Área** | **Meio** |
|---|---|---|---|
| **1** | Elaboração / Revisão | Gerência de Segurança da Informação | Sistema de Gestão de Documentos |
| **2** | Consenso | Gerência Corporativa de Contencioso e *Compliance* | Sistema de Gestão de Documentos |
| **3** | Consenso | Gerência Corporativa de Auditoria, Riscos e Controles Internos | Sistema de Gestão de Documentos |

| FASE | Atividade | Área | Meio |
|---|---|---|---|
| **4** | Consenso | Gerência Corporativa de Regulação da Distribuição e Transmissão | Sistema de Gestão de Documentos |
| **5** | Consenso | Gerência Corporativa de Governança de Dados e Gestão da Qualidade | Sistema de Gestão de Documentos |
| **6** | Validação de Conteúdo | Diretoria de Centro de Serviços Compartilhados | Através de e-mail com o “De Acordo”. |
| **7** | Aprovação | Conselho de Administração | Ata de Reunião |
| **8** | Aprovação para fins de liberação do documento no sistema | Superintendência de TI e TELECOM | Sistema de Gestão de Documentos |
| **9** | Divulgação | Gerência Corporativa de Desenvolvimento e Comunicação Interna | Canais de comunicação diversos. |

## 11. APROVAÇÃO

**ELABORADOR (ES) / REVISOR (ES)**

Selma Eduarda Neto – Governança de Centro de Serviços Compartilhados

Iris Cristina Ribeiro Silva – Gerência Corporativa de Contencioso e *Compliance*

Carina Natacha de Sousa Pires – Gerência Corporativa de Auditoria, Riscos e Controles Internos

Dayanni Rossi Grassano – Gerência Corporativa de Regulação da Distribuição e Transmissão

Erika Wilza Brito de Assis Lorenzo Alves – Gerente Corporativa de Contencioso e Compliance -

Comitê de Auditoria Estatutário.

**APROVADOR (ES)**

Tiago Barroso Oliveira – Superintendente de TI e TELECOM

Humberto Luiz Queiros Nogueira – Diretoria de Centro de Serviços Compartilhados

Conselho de Administração da Equatorial Energia S/A.