POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

REVISÃO 01.2023

1. FINALIDADE

Estabelecer princípios e diretrizes para a gestão estratégica da segurança da informação e cibernética a serem observados e aplicados de forma a salvaguardar as informações corporativas e demais ativos de informação, por meio do gerenciamento adequado dos riscos e suporte à manutenção dos negócios da Mata de Santa Genebra Transmissão S.A. (“MSG”), conforme os requisitos do negócio e de acordo com a legislação vigente.

2. CONCEITOS

2.1. Informação

Ativo, expresso de forma impressa, escrito em papel, armazenado digitalmente, transmitido por correio ou meios eletrônicos, mostrado em filmes, dialogado em palestras, postado em redes sociais, mídias sociais ou em reuniões formais ou informais, que necessita, por sua importância, ser adequadamente protegido, manuseado e gerenciado.

2.2. Segurança da Informação

Preservação da confidencialidade, integridade, disponibilidade, autenticidade, responsabilidade e confiabilidade.

2.3. Segurança Cibernética

Conjunto de diretrizes, instrumentos e ações que buscam proteger as informações e seus sistemas, os dispositivos e os ativos digitais da MSG, assegurando a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação da companhia.

2.4. Confidencialidade

Característica da informação que a torna reservada, com acesso por pessoas autorizadas.

2.5. Integridade

Característica da informação que a torna exata e completa.

2.6. Disponibilidade

Característica da informação que a torna acessível quando necessária em prazo compatível com o processo de negócio.

2.7. Rastreabilidade

Característica da informação que possibilita acompanhar ou identificar algo durante um processo: saber "o quê", "quem”, “quando”, “de onde" e "para onde”.

2.8. Dever de Diligência

Obrigação de ter o cuidado necessário na execução de ato ou procedimento, para que tudo se cumpra com regularidade.

2.9. Software Aplicativo

Programa de computador (normalmente referido apenas como aplicativo).

2.10. Proprietário da Informação
Diretor ou Coordenador que, por obrigação legal ou por delegação, é responsável pela informação.

2.11. Pessoa Autorizada
Pessoa que recebeu autorização, do proprietário da informação, para ter acesso a ela.

3. PRINCÍPIOS

3.1. **Confidencialidade:** garantir o acesso à informação unicamente às pessoas autorizadas, bem como resguardar as informações dadas em confiança e proteção contra a sua revelação a indivíduos, entidades ou processos não autorizados.

3.2. **Integridade:** salvaguardar a exatidão e completeza de ativos, visando protegê-lo, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais, bem como assegurar que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças.

3.3. **Disponibilidade:** garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3.4. **Rastreabilidade:** garantir o acompanhamento das operações nos processos da MSG, conforme mapeamento de criticidade, visando a identificação de qualquer tipo de alteração da informação.

3.5. **Privilégios mínimos:** garantir que as pessoas, os sistemas de informação e os processos acessem apenas as informações necessárias à execução de suas atividades.

3.6. **Exposição Mínima:** garantir que a informação deve ser mantida protegida, sendo exposta apenas quando necessária.

3.7. **Dever de Diligência:** todos os profissionais da MSG (administradores, coordenadores, estagiários e terceiros) são responsáveis pela preservação e pelo cumprimento da política de segurança cibernética da MSG, realizando todo acesso e uso da informação de forma responsável e regular.

3.8. **Conformidade:** garantir que os processos da MSG estejam de acordo com normas internas e externas, seguindo de forma rigorosa os protocolos exigidos em decorrência das atividades realizadas.

4. DIRETRIZES

4.1. Toda informação produzida ou incorporada pela MSG é de sua propriedade, sendo parte de seu patrimônio como ativo intangível e de uso exclusivo para o desenvolvimento de atividades MSG.

4.2. As informações tratadas, no âmbito da MSG, devem ser analisadas de forma ética, sigilosa e de acordo com as leis vigentes e normas internas, devendo ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada, evitando-se mau uso e exposição indevida.

4.3. As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades

relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

4.4. A MSG deverá adotar um modelo de **maturidade em segurança cibernética**, visando mitigar riscos e preservar as operações da Companhia, elevando continuamente os **níveis de segurança da informação.**

4.5. **Os ativos digitais** de propriedade da MSG ou contratados para serem utilizados pela Companhia, **devem ser protegidos** de forma compatível com a criticidade e relevância de seus negócios, com o estabelecimento de **controles de segurança** como parte integrante do processo de desenvolvimento, aquisição e vida útil dos aplicativos para assegurar que as informações processadas estejam **protegidas**, de acordo com a **classificação e exposição a risco**.

4.6. Os processos e sistemas de informação devem atender às **exigências de rastreabilidade** para alterações e acessos às informações e quando do desenvolvimento e/ou aquisições de aplicativos.

4.7. Os equipamentos de informática e comunicação, sistemas, informações e acessos são utilizados para a realização das atividades profissionais, mediante utilização de senha individual e secreta, que será utilizada como assinatura eletrônica e vedado seu compartilhamento, para o desenvolvimento de um ambiente organizacional que permita à MSG identificar e **gerenciar o risco de segurança cibernética**, no que tange a sistemas, processos, pessoas, ativos, dados e recursos.

4.8. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, independente do cargo, função ou local de trabalho, para que seja responsabilizado por suas ações, pelo descumprimento ou violação da presente política, em acordo com as normativas internas e externas vigentes.

4.9. Os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras, devendo ser feita a **gestão e revisão das identidades** e dos acessos aos recursos computacionais da MSG, garantindo a **definição de privilégios mínimos** e **rastreabilidade** de acessos realizados, com o **gerenciamento das vulnerabilidades** para manutenção das tecnologias devidamente atualizadas, revisadas e testadas.

4.10. A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas, para que a MSG possa administrar, monitorar e proteger contra acessos não autorizados às redes e aplicativos prioritários.

4.11. A **cultura de segurança cibernética** deve ser desenvolvida por meio da conscientização dos administradores, coordenadores, estagiários e terceiros, com disponibilização de meio para detecção e comunicação dos riscos à área de segurança da informação.

4.12. Serão desenvolvidas e implementadas **atividades apropriadas** para agir contra um **incidente de segurança cibernética detectado**, assim como **planos de resiliência** a fim de **restaurar** quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética.

4.13. Os níveis de segurança da informação deverão ser estabelecidos em regulamentos específicos a serem aprovados pela Diretoria Reunida da MSG.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

REVISÃO 01.2023

5. DISPOSIÇÃO FINAL

5.1. São responsáveis pela observância desta Política os diretores, coordenadores e prestadores de serviço.

5.2. As violações ou incidentes de segurança da informação devem ser informadas à Coordenadoria Administrativa da MSG.

5.3. Toda violação ou desvio deve ser investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

5.4. A MSG reserva-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em eventuais processos investigatórios, adotar as medidas legais cabíveis e punir os infratores, no caso de uso indevido de recursos.

5.5. Deverão ter ciência sobre esta Política em, no máximo 30 (trinta) dias após a sua data de aprovação, todos os coordenadores, prestadores de serviço e administradores da MSG.

5.6. Todos os colaboradores e prestadores de serviço deverão fazer adesão ao acordo de confidencialidade ou Cláusula de confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

5.7. As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas da MSG e na legislação vigente no Brasil.

5.8. Os casos omissos relativos a esta Política deverão ser encaminhados para análise da Coordenadoria Administrativa.

6. LEGISLAÇÃO E NORMAS RELACIONADAS AO ASSUNTO

6.1. Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados;

6.2. Resolução Normativa ANEEL nº 964/2021

6.3. Código de Conduta, Ética e Integridade da MSG;

6.4. NPC 0301 Política de Segurança da Informação e Cibernética – Tecnologia da Informação COPEL (versão 13 de 15/06/2022).

A revisão desta Política foi aprovada na Reunião de Diretoria 003/2024 de 16.01.2024 e na 199ª Reunião do Conselho de Administração de 25.01.2024.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

REVISÃO 01.2023

ANEXO I

TERMO DE CONFIDENCIALIDADE

1. São consideradas informações confidenciais (“Informações Confidenciais”), para os fins deste Termo:

a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da MSG e a seus sócios ou clientes, independente destas informações estarem contidas em qualquer tipo de mídia ou em documentos físicos.

a) Informações acessadas em virtude do desempenho de suas atividades na MSG, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto aos administradores da MSG, acionistas, funcionários, estagiários ou terceirizados, clientes, fornecedores e prestadores de serviços em geral.

2. Estou ciente de que todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive minutas de contrato, cartas, apresentações, e-mail e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos elaborados ou obtidos em decorrência do desempenho das minhas atividades na MSG são e permanecerão sendo propriedade exclusiva da MSG.

3. Comprometo-me a utilizar as Informações e documentos a que vir a ter acesso estrita e exclusivamente para desempenho de minhas atividades na MSG, e a não divulgar tais Informações e documentos para quaisquer fins que não o desempenho de minhas atividades na MSG, devendo todos os documentos permanecer em poder e sob a custódia da MSG.

4. Este Termo é parte integrante das regras que regem a relação entre as partes e, ao assiná-lo, aceito expressamente os termos e condições aqui estabelecidos.

Local, (data).

_____

Assinatura

(Nome completo)