Essentia Energia

POL.TI.01

Política de Segurança Cibernética

Sumário

POLÍTICA DE SEGURANÇA CIBERNÉTICA
ESSENTIA ENERGIA

1. INTRODUÇÃO

A Essentia Energia e suas subsidiarias, estão comprometidas em assegurar a disponibilidade, a integridade e a confidencialidade das informações que lhe foram confiadas pelas partes interessadas, incluindo direção, empregados, entidades setoriais e outros parceiros de negócios.

A Política de Segurança Cibernética estabelece os princípios e o marco para controle e gestão de riscos derivados de ameaças e vulnerabilidades dos sistemas de controle ou sistemas de informação e comunicações da empresa, incluindo todos os ativos que fazem parte da infraestrutura cibernética do Grupo e os ativos de informação.

2. VÍNCULOS

1.1 POL-TI-02 - Estatuto do Comitê de Segurança Cibernética

1.2 POL-TI-03 – Gestão de Acessos

3. OBJETIVO

Garantir a confidencialidade, integridade e disponibilidade de todos os ativos digitais e informações relacionadas à geração de energia da empresa, prevenindo, detectando, respondendo e reduzindo vulnerabilidades a incidentes cibernéticos, de forma a minimizar riscos e assegurar a continuidade dos negócios.

A alta direção, em alinhamento com as políticas globais da empresa, reafirma seu compromisso em adotar medidas para mitigar eventuais ocorrências que comprometam a segurança das informações sob sua posse ou responsabilidade; prevenir e reduzir possíveis incidentes relacionados às interfaces tecnológicas com seus stakeholders; e promover a disseminação da cultura de cibersegurança e das boas práticas entre todos os colaboradores.

4. ESCOPO

Esta política aplica-se a todos os funcionários, contratados e terceiros que tenham acesso aos ativos digitais e às informações da empresa, bem como aos dispositivos, sistemas e redes que dão suporte às suas atividades. Abrange também o desenvolvimento de sistemas de informação e a adoção de novas tecnologias utilizadas nas operações da organização.

5. GOVERNANÇA

A governança da segurança cibernética na empresa é estruturada para assegurar que as responsabilidades, funções e decisões sejam bem definidas e alinhadas aos objetivos estratégicos e regulatórios. Essa estrutura busca garantir a aplicação eficaz da Política de Segurança Cibernética, promover a conformidade legal e regulatória e assegurar a melhoria contínua das práticas e controles relacionados à proteção dos ativos digitais e operacionais da organização.

5.1 Comitê de Segurança Cibernética

Equipe multidisciplinar que tem como objetivo atuar na governança da segurança digital da Essentia, definindo diretrizes, políticas e prioridades que alinhem a proteção da informação aos objetivos estratégicos do negócio. Ele reúne representantes de áreas críticas para avaliar riscos, aprovar investimentos, monitorar conformidade regulatória, acompanhar incidentes relevantes e promover a cultura de segurança entre os colaboradores, garantindo uma visão integrada e estratégica da cibersegurança. Mais detalhes podem ser consultados na política específica, POL-TI-02 - Estatuto do Comitê de Segurança Cibernética

5.2 Gerente de Segurança Cibernética

O gerente de TI & TO atua como gerente de segurança cibernética, liderando a equipe responsável pela proteção dos ativos digitais e operacionais da empresa. Suas atribuições incluem coordenar a execução da Política de Segurança Cibernética, supervisionar as iniciativas de prevenção e resposta a incidentes e apoiar a implementação de controles e melhorias contínuas.

5.3 Gerente Regulatório

O gerente da área Regulatória é responsável por assegurar que a empresa esteja em conformidade com todas as leis, normas e regulamentos relacionados à segurança cibernética no setor elétrico, monitorando alterações legislativas e garantindo a atualização dos processos internos.

6. ARQUITETURA

As redes devem ser segregadas em níveis de segurança, de acordo com a sua função:

- *Corporativa*: ambiente onde se encontram estações de trabalho, impressoras e demais equipamentos de escritório. Não deve possuir qualquer conexão com o ambiente operacional.
- *DMZ*: redes intermediárias que fazem a interface entre os ambientes operacionais e os ambientes externos. Nesse nível, encontram-se gateways de comunicação responsáveis por coletar ou concentrar informações das redes operacionais e distribuí-las para aplicações externas, mantendo controles rígidos de acesso e filtragem de dados.
- *Operacional*: redes de nível mais baixo nas instalações, onde estão conectados os IEDs, câmeras, medidores e demais dispositivos do ambiente de TO (Tecnologia Operacional). Podem existir servidores e aplicações para uso e acesso local. Este nível não deve possuir qualquer comunicação direta com redes ou ambientes externos, garantindo isolamento e segurança.

A segregação entre cada nível deve ser realizada por um firewall, e os ambientes devem ser possuir solução antimalware.

7. GESTÃO DE ACESSOS

O direito de acesso deverá seguir o princípio do privilégio mínimo, garantindo que cada usuário tenha acesso apenas aos recursos estritamente necessários para a execução de suas atividades.

Os detalhes sobre os fluxos de solicitações e revogações de acesso aos ambientes digitais de empresa, informações sobre credenciais de acesso para colaboradores e terceiros podem ser consulado na política específica, POL-TI-03 – Gestão de Acessos.

8. GESTÃO DE ATIVOS

Os ativos digitais devem ser utilizados de forma responsável, assegurando a integridade das informações e a disponibilidade dos equipamentos nas instalações. Cabe à equipe de TI planejar, implementar e manter soluções de segurança cibernética que protejam esses ativos e garantam sua disponibilidade, bem como estabelecer um processo eficaz de gestão de ativos, com registro, revisão e validação periódica dos inventários, visando otimizar seu valor, utilização e desempenho ao longo de todo o ciclo de vida, em conformidade com as diretrizes de uso e manutenção da empresa.

8.1 Inventário

Os inventários de softwares e hardwares, devem ser atualizados a cada 24 meses e armazenado via ferramenta de compartilhamento de arquivos utilizada pela empresa. Os inventários devem ser considerados dados Internos, e tratados como tal. Devem ter acesso ao inventário de ativos apenas a equipe de TI, para os ativos corporativos, e as equipes de TI e operações, para os equipamentos operacionais.

8.2 Hardening

Devem existir baselines de configuração dos ativos digitais. As baselines são atualizadas sob demanda, sempre que houver alguma reavaliação de riscos, vulnerabilidades ou políticas. Sempre que aplicável, os ativos devem dispor de agentes capazes de refletir as configurações de Hardening e gerar alertas sobre quaisquer não conformidades.

Todos os ativos novos devem utilizar, automaticamente, as versões mais recentes do baseline.

9. VULNERABILIDADES

A identificação de vulnerabilidades é executada de forma automatizada ou manual, podendo ser executada pela própria empresa ou por terceiro especializado e contratado para esta atividade. O resultado desta varredura deve conter as vulnerabilidades identificadas, classificadas em criticidade, de acordo com o potencial impacto de sua exploração.

Nível	Critério
Crítico	Afeta sistemas ou equipamentos críticos com impacto total na disponibilidade; risco direto à segurança das pessoas; redução da vida útil dos equipamentos; vazamento de dados sensíveis com potencial de danos à imagem e reputação; possibilidade de afetar terceiros e parceiros.
Alto	Afeta sistemas importantes com impacto parcial na disponibilidade; risco de alteração ou exploração de dados sensíveis; possibilidade de anular medidas de segurança.
Médio	Não afeta ativos críticos ou possui exploração difícil; baixo impacto na disponibilidade e na preservação de equipamentos.
Baixo	Pouco ou nenhum impacto na segurança, disponibilidade ou preservação; dano potencial limitado ou de exploração muito difícil; sem impacto nos negócios; sem acesso a dados sensíveis.

10. ATUALIZAÇÕES

A aplicação de atualizações nos ativos digitais visa corrigir vulnerabilidades, falhas funcionais e aprimorar recursos e segurança de softwares, sistemas operacionais e firmwares. As atualizações devem ser planejadas para causar o menor impacto possível nas operações, sendo aplicadas preferencialmente em janelas de manutenção e após avaliação da necessidade. Ativos cruciais para a operação, que exijam alta disponibilidade, não devem utilizar atualizações automáticas. Para estes casos, as atualizações devem ser estudadas individualmente, e devem ser realizadas apenas em caso de necessidade de novas funcionalidades do negócio, ou risco grave à cibersegurança.

Todos os ativos novos devem utilizar as versões mais atualizadas, antes da entrada em operação. Podem ser criadas exceções para casos de substituições de ativos, caso a versão mais atualizada seja incompatível com o sistema em uso.

11. CLASSIFICAÇÃO DE DADOS E INFORMAÇÕES

Toda informação deve ser classificada em níveis de confidencialidade, de acordo com o impacto relacionado à quebra de confidencialidade. Para cada nível, devem ser aplicadas restrições de acesso específicas.

Nível	Impacto	Restrições de acesso
Confidencial	O acesso não autorizado à informação pode causar danos severos aos negócios ou à reputação da organização.	A informação é disponibilizada somente para colaboradores autorizados, e em caso de atendimento a demandas judiciais ou órgãos reguladores. As informações classificadas neste nível deverão ter indicação clara de quem está autorizado a acessá-las.
Interna	O vazamento de dados internos pode causar danos pontuais ou inconveniências à organização.	A informação é disponibilizada internamente a colaboradores ou órgãos reguladores.
Pública	Sem impacto	A informação está disponível para o público em geral

12. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

São considerados incidentes de segurança da informação quaisquer ocorrências que comprometam o ambiente de tecnologia, afetando a confidencialidade, disponibilidade, integridade, autenticidade ou auditabilidade dos ativos da empresa

12.1 Classificação dos Incidentes de Segurança da Informação

Os incidentes devem ser classificados considerando seu impacto nas operações.

Nível	Critério
Crítico	Possibilidade, direta ou indireta, de risco à vida ou aos ativos da empresa. Possibilidade de ocasionar indisponibilidade dos ativos e consequente perda financeira, multas, ou qualquer risco de impactos financeiros significativos. Risco de disponibilidade e integridade, interna e externa, dos recursos tecnológicos, bem como também a imagem da empresa. Risco de que o sigilo de informações tenha sido comprometido. Necessidade de comunicação externa à fornecedores ou órgãos reguladores.
Alto	Prejuízo parcial à disponibilidade e integridade dos recursos tecnológicos e à imagem da Empresa, porém as operações externas com órgãos reguladores continuem operacionais e não tenham sido afetadas. O sigilo de informações sensíveis está preservado, mas pode haver risco de comprometimento. Não há necessidade de comunicação externa ou a órgãos reguladores.
Médio	A operação diária não tenha sido afetada, mas que necessite de atuação imediata para que o incidente não se agrave ou se propague. O sigilo de informações está preservado. Não existe impacto financeiro evidente ou significativo. O incidente está controlado, mas deve ser monitorado.
Baixo	Pequeno impacto coletivo ou departamental, considerado caso isolado. Não oferece risco ao sigilo de informações ou disponibilidade de recursos. Baixo risco funcional e financeiro.

12.2 Identificação de Incidentes

Todos os dispositivos digitais devem estar configurados para gerar logs de sistemas, que possam ser utilizados tanto para identificação dos incidentes de segurança da informação, quanto para análises e investigações posteriores. Os logs devem ser armazenados pelo período mínimo de um mês.

Todo incidente que coloque em risco a segurança da Informação, deve ser reportado imediatamente à equipe de TI através do e-mail ti@essentiaenergia.com.br e para os contatos do anexo I, para avaliação da situação e adoção das medidas necessárias.

12.3 Registros de Incidentes de Segurança da Informação

A empresa deverá registrar detalhadamente todos os incidentes cibernéticos de maior impacto, incluindo aqueles envolvendo informações recebidas de empresas prestadoras de serviços terceirizadas.

Para cada incidente registrado, será realizada uma análise minuciosa da causa raiz e dos impactos operacionais, financeiros, de segurança e reputação decorrentes do evento.

Com base nessa análise, deverão ser implementados controles e ações corretivas eficazes para mitigar os efeitos do incidente, prevenir recorrências e garantir a continuidade das atividades essenciais da organização.

A gestão desses processos deve ser documentada e acompanhada por equipes responsáveis, assegurando a transparência e a rastreabilidade em todo o ciclo de vida do incidente.

12.4 Notificação de Incidentes Cibernéticos

Os incidentes de segurança da informação devem ser reportados imediatamente aos responsáveis designados pela empresa, seguindo a ordem de escalonamento definida no Anexo I. A empresa deverá notificar os órgãos setoriais competentes tão logo o incidente seja identificado. Durante todo o processo de resposta, deverão ser registradas e preservadas informações relevantes que subsidiem a elaboração de relatórios detalhados de análise forense após a ocorrência.

13. TREINAMENTOS

A equipe de TI deve fornecer treinamento periódico sobre segurança cibernética para todos os funcionários, contratados e parceiros da empresa, visando disseminar a cultura de segurança cibernética da empresa.

O treinamento deve abordar boas práticas de segurança cibernética, como senhas seguras, proteção de dados e reconhecimento de ataques de *phishing* (exemplos).

A última versão do treinamento de segurança cibernética faz parte do pacote de *onboarding* de novos funcionários da Essentia.

14. AUDITORIA

O ambiente de tecnologia da empresa deverá ser submetido a auditoria anual de segurança cibernética. O framework adotado deve estar alinhado às atividades e necessidades da empresa, garantindo aderência às melhores práticas do setor. O processo de auditoria poderá ser conduzido por equipes internas ou por prestadores de serviços externos especializados.

15. SIMULAÇÃO DE AMEAÇAS

A empresa deverá executar ao menos um teste anual de incidentes de informação, contemplando simulações de cenários de interrupção capazes de impactar diretamente as atividades prestadas pela empresa.

Todos os setores que apoiam a prestação dos serviços — incluindo áreas de TI, fornecedores e parceiros estratégicos — deverão participar dos exercícios. Cada simulação deve reproduzir falhas em sistemas críticos e avaliar a capacidade de resposta e recuperação, assegurando a manutenção da operação e a continuidade dos serviços.

Ao término de cada teste, será elaborado um relatório contendo a análise de desempenho das equipes, o tempo de recuperação dos sistemas, o impacto nos serviços e as não conformidades observadas.

As falhas e dificuldades identificadas deverão ser tratadas por meio de ações corretivas, e os procedimentos envolvidos deverão ser atualizados para incorporar as melhorias necessárias, garantindo a evolução contínua da resiliência operacional da organização.

16. ELABORAÇÃO, REVISÃO E APROVAÇÃO

Nome	Função	Atividade	Assinatura
Adrisson Consoni Floriano	Gerente de Elaborador IT/OT	Elaboração	Signed by: Adrisson Floriano C1F67E962241431...
Hudson Souza	Gerente de O&M	Revisão	DocuSigned by: Hudson Souza CB7EDF8GE3AB4C5...
Gilberto Peixoto	Diretor de Implantação O&M	Aprovação	Assinado por: C08C474BC6CC42A...

17. HISTÓRICO DE REVISÕES

Revisão	Data	Responsável	Observações
1.0	06/08/2025	Adrisson Consoni Floriano	Emissão inicial do documento

ANEXO 1 - Escalonamento de acionamentos para incidentes de segurança de informação

Nome	Função	E-mail	Telefone
André Felipe Alves	Analista de TO	andre.alves@essentiaenergia.com.br	(84) 99211-5422
Gabriel Batista	Analista de TI	gabriel.batista@essentiaenergia.com.br	(11) 95154-8309
Adrisson Consoni Floriano	Gerente de Tecnologia IT/OT	adrisson.floriano@essentiaenergia.com.br	(48) 99695-2570
Hudson Souza	Gerente de O&M	hudson.souza@essentiaenergia.com.br	(11) 99688-6347
Gilberto Peixoto	Diretor de Implantação O&M	gilberto.peixoto@essentiaenergia.com.br	(11) 99369-0226