Política de Governança Corporativa

PGC-08-010-R01 – Política Externa de Segurança da Informação e Resposta a Incidentes no Monitoramento de Mercado

grupo

Política externa

assunto

Política Externa de Segurança da Informação e Resposta a Incidentes no Monitoramento de Mercado

código

PGC-08-010-R01

vigência

10/10/2025

disclamer

O presente documento é de uso exclusivamente interno da CCEE – Câmara de Comercialização de Energia Elétrica e contém informações específicas ao processo interno que o intitula. Seu propósito é apoiar e esclarecer todos os usuários envolvidos no processo, sobre quais as regras definidas e aprovadas para cumprimento e conformidade.

Grupo: Governança Corporativa **Vigência:** 10/10/2025
Assunto: Política Externa de Segurança da Informação e Resposta a Incidentes no Monitoramento de Mercado **Código:** PGC-08-010-R01

1. objetivo

A Câmara de Comercializadora de Energia Elétrica (CCEE) reforça seu compromisso formal com a implementação rigorosa de processos e controles destinados a assegurar a proteção das informações e mitigar os riscos e ameaças relacionados à Segurança da Informação.

2. princípios

Em conformidade com a Política de Segurança de Informação da CCEE, nossas práticas estão fundamentadas em quatro princípios essenciais:

- **Confidencialidade:** Aplicamos todos os esforços para garantir que os dados obtidos sejam mantidos em confidencialidade, evitando acesso, uso indevido ou qualquer vazamento dessas informações**.**
- **Integridade:** Asseguramos que o conteúdo das informações não seja indevidamente alterado ou violado.
- **Disponibilidade:** Aplicamos todos os esforços para garantir que as informações e os recursos tecnológicos estejam sempre acessíveis quando necessário.
- **Autenticidade:** Certificamos que as informações provêm das fontes anunciadas, garantindo sua origem legítima.

3. diretrizes

Este documento apresenta uma visão geral e abrangente das principais estratégias de Segurança da Informação adotadas pela CCEE. Seu objetivo é salvaguardar nossos ativos tecnológicos e informações vitais.

4. disposições gerais

Este segmento estabelece práticas que se aplicam a toda a CCEE, incluindo a área de monitoramento de mercado. São diretrizes aplicadas observando o nível de segurança nos sistemas de informação requerido, a complexidade, os custos, probabilidade, impacto e extensão:

- **PROTEÇÃO DA INFORMAÇÃO**

Independentemente da forma – seja eletrônica, escrita ou verbal – e do modo de compartilhamento, armazenamento ou transmissão, as informações devem ser usadas exclusivamente para os fins autorizados pelos gestores de informação. Qualquer uso não autorizado é estritamente proibido.

- **CONTROLE DE ACESSOS E RASTREABILIDADE**

O acesso às informações está restrito às pessoas autorizadas e é continuamente rastreado, garantindo a transparência e a responsabilização em todas as interações.

- **PREVENÇÃO CONTRA VÍRUS E SOFTWARES MALICIOSOS**

Implementamos rigorosos controles para prevenir a entrada e a disseminação de vírus, arquivos e softwares maliciosos em nossa rede e sistemas de informação. A instalação e uso de arquivos e softwares não homologados são proibidos, sendo reforçados por nosso sistema de Firewall.
Com estas práticas e diretrizes robustas, a CCEE reafirma seu compromisso inabalável com a Segurança da

Informação, salvaguardando não apenas nossos dados, mas também a confiança que nossos stakeholders depositam em nós.

- **MANUTENÇÃO E BACKUP SEGURO**

Implementamos procedimentos específicos para assegurar a recuperação eficiente de dados e informações quando necessário. Isso inclui robustos protocolos de manutenção e backups regulares, garantindo a resiliência dos nossos sistemas.

- **CLASSIFICAÇÃO DE DADOS E INFORMAÇÕES**

Para uma gestão eficaz, a CCEE classifica suas informações em quatro categorias: Pública, Interna, Restrita e Confidencial, permitindo um controle claro sobre o acesso e o compartilhamento de dados confidenciais e dados pessoais e/ou sensíveis.

- **CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS**

Comprometidos com a confidencialidade, integridade, disponibilidade e autenticidade das informações, a CCEE promove uma cultura de Segurança da Informação e Privacidade. Através de treinamentos especializados, nossos colaboradores, prestadores de serviços e estagiários são capacitados, reforçando a grande importância desses princípios.

- **CONFIDENCIALIDADE GARANTIDA**

A CCEE adota as medidas necessárias para garantir a confidencialidade das informações com seus Parceiros de Negócios, reforçando o compromisso inabalável com a proteção dos dados de nossos clientes e demais parceiros.

- **USO RESPONSÁVEL DOS RECURSOS DE INFORMAÇÃO**

A CCEE estabelece diretrizes rigorosas para o uso de softwares e equipamentos, permitindo apenas o uso de tecnologias configuradas de acordo com nossos padrões organizacionais. Isso garante a segurança e integridade e disponibilidade dos dados em todas as interações.

- **PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES**

Nossos controles e políticas são meticulosamente desenvolvidos para prevenir vazamentos de informações. Estas medidas incluem práticas sólidas para o uso de correio eletrônico, acesso à internet, conexões remotas e dispositivos móveis. Além disso, orientamos nossos colaboradores, prestadores de serviços e estagiários sobre comportamentos seguros, tanto em locais públicos quanto durante interações com fornecedores, assegurando a confidencialidade em todas as etapas.

Quando do ingresso de novos colaboradores na área de monitoramento, devem ser disponibilizados os normativos internos para que sejam difundidas as boas práticas entre os colaboradores e adesão a termo específico de responsabilidade.

- **DESENVOLVIMENTO SEGURO**

Nossos sistemas de informação são desenvolvidos de acordo com critérios e procedimentos adequados para a segurança e privacidade em cada etapa do processo. Além disso, todas as aquisições de softwares ou serviços em soluções SaaS (Software as a Service), são submetidas a uma avaliação para garantir que atendam aos requisitos de segurança estabelecidos internamente na CCEE.

Além das práticas já estabelecidas para a CCEE o Monitoramento de Mercado conta com um ambiente de computação confidencial para recebimento de informações dos agentes, mantém as informações criptografadas e sem qualquer interação humana em todo o seu ciclo de vida.

- **GESTÃO E DETECÇÃO DE VULNERABILIDADES**

Dedicamos especial atenção à gestão e detecção de vulnerabilidades. Implementamos estratégias avançadas para identificar e corrigir potenciais pontos fracos em nossos sistemas, garantindo assim uma defesa robusta contra ameaças cibernéticas.

Na CCEE, contamos com uma variedade de componentes de segurança operando nas fronteiras das comunicações internas e externas. Estes componentes são projetados para evitar a intrusão na rede. Além disso, empregamos ferramentas avançadas de gestão de vulnerabilidades.

No contexto da computação confidencial, mecanismos de controles são necessários, testes de penetração (pentests), avaliações de vulnerabilidades de código e auditorias baseadas em controles anualmente. Essas práticas garantem uma abordagem proativa para identificar e corrigir possíveis brechas, reforçando assim nossa postura de segurança de forma contínua e robusta.

- **ANTECIPAÇÃO DE AMEAÇAS E ATAQUES CIBERNÉTICOS E TESTES DE INVASÃO**

Nossa abordagem proativa inclui a antecipação de ameaças e ataques cibernéticos. Realizamos regularmente testes de invasão para avaliar nossa resistência a possíveis ataques, garantindo que estejamos sempre um passo à frente dos adversários. Essas medidas são fundamentais para manter a segurança e a integridade de nossos sistemas, protegendo assim as informações sensíveis da organização.

- **TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

A CCEE possui uma infraestrutura robusta para prevenir ameaças cibernéticas. Qualquer incidente de segurança cibernética é minuciosamente analisado e classificado conforme seu impacto, que varia entre o risco real ao potencial, garantindo uma resposta adaptada à gravidade da situação.

- **INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

É caracterizado um incidente de segurança da informação quando há uma ocorrência que indica possível violação da confidencialidade, integridade ou disponibilidade de informações e sistemas. Esses incidentes podem ser classificados como:

  - Ataque Externo: Acesso não autorizado aos sistemas da CCEE por parte de agentes externos.
  - Código Malicioso: Software desenvolvido para prejudicar sistemas, roubar dados ou causar danos.
  - Uso Não Autorizado de Ativo: Utilização indevida de recursos sem permissão, resultando em violação de políticas.
  - Acesso Não Autorizado: Entrada não permitida de um usuário a informações confidenciais sem devida autorização.
  - Indisponibilidade de Serviço: Situação em que um serviço ou sistema não está acessível, interrompendo operações normais.
  - Fraude: Ação intencional e enganosa para obter vantagem ilegal, prejudicando terceiros ou organizações.
  - Vazamento de informações: Refere-se à divulgação não autorizada de dados pessoais e/ou sensíveis ou informações confidenciais, seja por erro humano ou atividade maliciosa. A CCEE possui um protocolo rigoroso para identificar, conter e remediar vazamentos. Isso inclui uma análise minuciosa das vulnerabilidades, a aplicação imediata de medidas corretivas e uma comunicação transparente com todas as partes envolvidas, assegurando uma resposta rápida e eficaz para proteger a integridade e confidencialidade das informações da organização.

São exemplos de possíveis ocorrências no processo de monitoramento:

- Envio de e-mails ou tarefas sistêmicas para agentes indevidos;
- Publicação de informações incorretas ao mercado;
- Citação de outros agentes em comunicações do monitoramento;
- Disponibilização de acessos indevidos a usuários não pertencentes ao monitoramento;
- Incidentes de segurança da informação são caracterizados também como incidentes de privacidade quando há dados pessoais envolvidos e, portanto, são abarcados pela Lei Geral de Proteção de Dados (LGPD).

5. processo em caso de incidente

- **ATORES E RESPONSABILIDADES**

  - Notificador: pessoa ou sistema de monitoração que notifica o incidente. Pessoas externas à CCEE devem utilizar o canal monitoramento@ccee.org.br;

  - Acionador(es): responsável pelo recebimento das notificações e pela condução do incidente quando não envolver problemas sistêmicos, no caso, a equipe de monitoramento;

  - Equipe de Prevenção e Resposta a Incidentes (EPRI): acionada somente quando houver impacto em sistemas e constituída por membros da Gerência Executiva de Governança Corporativa – Segurança da Informação (GEGOI), Gerência Executiva de Suporte e Infraestrutura (GESIN) e Gerência de Segurança de Mercado (GSEM).

- **IDENTIFICAÇÃO**

Ao identificar um incidente de segurança da informação, o Acionador deverá reportar o ocorrido ao gestor imediato, este incidente será tempestivamente analisado pelo gestor, o qual avaliará a necessidade de acionamento da EPRI.

Com a necessidade de acionar a EPRI, o Acionador deverá abrir uma ocorrência na Central de Serviços | Segurança da Informação, identificando qual o tipo de incidente, informando:

- Descrição do ocorrido, incluindo indicação da informação e/ou sistema afetados;
- Levantamento da quantidade de clientes potencialmente afetados;
- Detalhamento dos processos e repositórios que utilizaram ou armazenaram a informação a fim de auxiliar na rastreabilidade dos acessos e possíveis pontos de falha;

As áreas que precisem ser envolvidas no incidente não terão acesso a qualquer informação do monitoramento e assinará termo específico para o seu envolvimento nos incidentes cobertos pela presente Política, nos moldes do termo específico existente para a área de monitoramento.

- **AVALIAÇÃO**

O Acionador deverá fazer a avaliação preliminar ou indicar a necessidade de composição da EPRI para realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes. Em sendo

desnecessária a composição da EPRI, o Acionador assumirá as fases descritas no fluxo do processo.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas/processos que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.

Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para trâmites regulares da área de monitoramento.

A criticidade do incidente pode ser definida de acordo com o volume de dados expostos em relação à sensibilidade de tais dados, dentre outros critérios a serem avaliados pela EPRI.

A EPRI deve, no mínimo:

- Identificar a causa raiz do incidente;
- Rastrear endereços IP e acessos envolvidos;
- Rastrear transações e transferências de dados irregulares;
- Identificar métodos de acesso e vulnerabilidades exploradas;
- Entrar em contato com os responsáveis pelos sistemas afetados para assistência na avaliação.

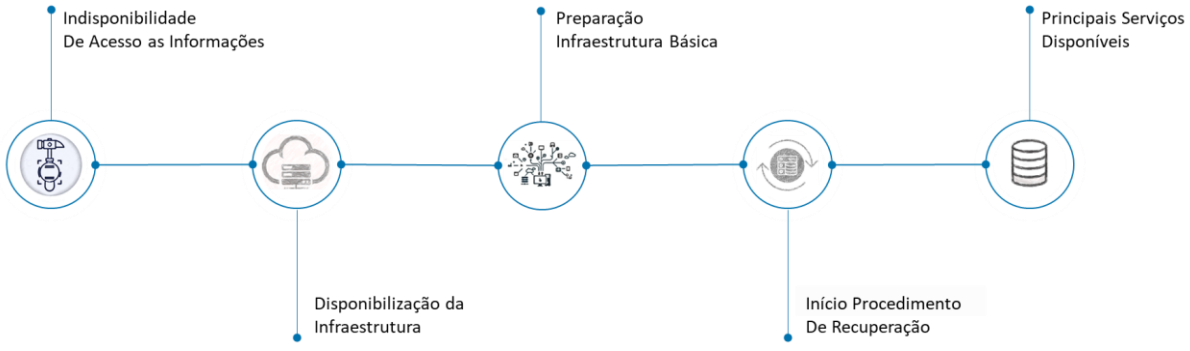
- **CONTENÇÃO E ELIMINAÇÃO**

A fim de limitar o dano e isolar os sistemas afetados podem ser necessárias medidas de contenção e eliminação, que podem ensejar a suspensão de aplicações ou o desligamento de sistemas, sem que sejam perdidas evidências necessárias para investigação do incidente.

Em se tratando de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos envolverão questões disciplinares, o que inclui a demissão por justa causa.

- **RECUPERAÇÃO**

O processo de recuperação de sistemas, após indisponibilidade, consiste no seguinte fluxo a seguir, que possui a duração aproximada de 8 horas.



- **COMUNICAÇÃO**

Quando o incidente de vazamento de dados envolver dado(s) confidencial(is) do(s) agente(s), este deve ser imediatamente comunicado ao(s) agente(s) afetado(s) e à ANEEL. Caso o incidente não envolva dado(s) confidencial(is) do(s) agente(s), o incidente deve ser reportado à ANEEL.

São exemplos de dados confidenciais dos agentes aqueles que são objeto do monitoramento intensivo ou aleatório (informações comerciais disponibilizadas ao monitoramento, preços, contrapartes e montantes contratados), que são objeto de criptografia por computação confidencial (preço, marcação a mercado das 5 maiores contrapartes) e resultado da Análise de Risco Integrada.

Quando o incidente de segurança se caracterizar também como incidente de privacidade, as divulgações devem seguir o artigo 48 da LGPD.

- **LIÇÕES APRENDIDAS**

Após a avaliação pela equipe, devem ser apresentadas ao Conselheiro responsável pelo Monitoramento de Mercado as lições aprendidas incluindo:

- Proposta de medidas que podem ser adotadas para que não haja novas ocorrências;
- Tempo consumido/prazo estimado para que essas medidas sejam adotadas.

6. atribuições e responsabilidades

GSEM – GERÊNCIA DE SEGURANÇA DE MERCADO

- Reportar ocorrência de possível incidente de segurança da informação ao gestor imediato assim que identificada;
- Mapear a ocorrência para identificar os impactos e potenciais agentes envolvidos;
- Elaborar um plano de ação para mitigar os impactos e adotar ações corretivas.

GEGOI – GERÊNCIA EXECUTIVA DE GOVERNANÇA INSTITUCIONAL

- Analisar e avaliar os casos de violações, vazamentos, incidentes e demais eventos negativos relativos à Segurança da Informação na CCEE, conforme Política de Segurança da Informação da CCEE.

GESIN – GERÊNCIA EXECUTIVA DE SUPORTE E INFRAESTRUTURA

- Avaliar, monitorar, documentar e agir perante os incidentes de segurança da informação ou possíveis ameaças com a formalização de procedimentos para assegurar respostas rápidas, efetivas e ordenadas, acionando a área impactada/responsável quando necessário, conforme Política de Segurança da Informação da CCEE.