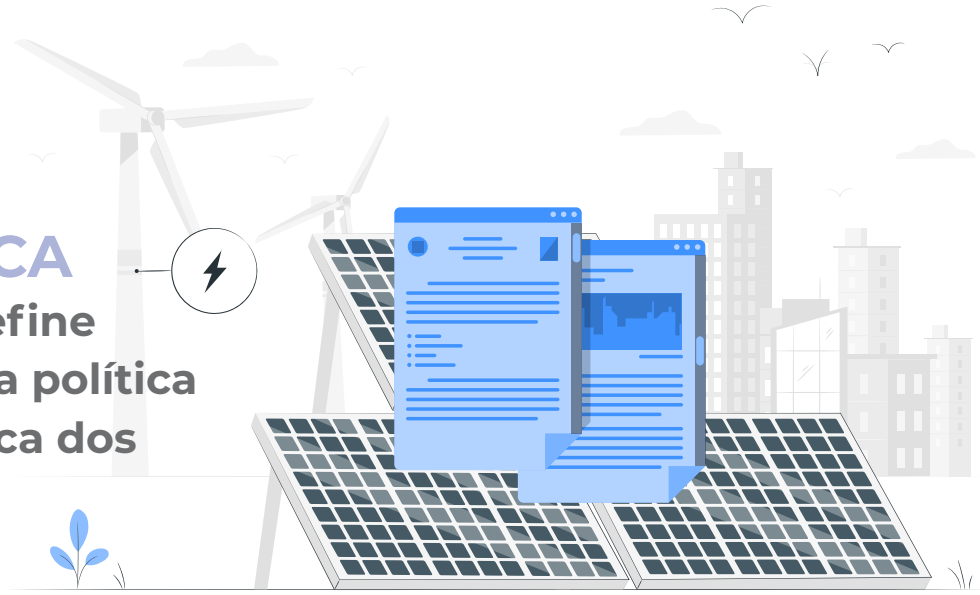
OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF



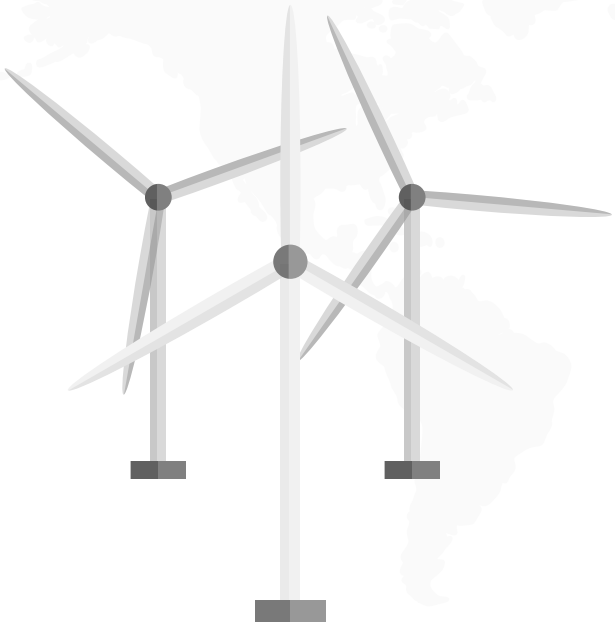
ENERGIA ELÉTRICA

Resolução da ANEEL define diretrizes e conteúdo da política de segurança cibernética dos agentes do setor

A Resolução Normativa nº 964, de 14 de dezembro de 2021, da Agência Nacional de Energia Elétrica (ANEEL), que entrará em vigor no dia 1º de julho de 2022, estabelece as diretrizes e o conteúdo mínimo das políticas de segurança cibernética dos agentes do setor de energia elétrica.

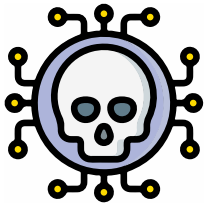
Objetivo da Resolução

Fixar diretrizes e conteúdo mínimo que devem ser adotados nas políticas de segurança cibernética dos agentes do **setor de energia elétrica**:



- Concessionários
- Permissionários
- Autorizados de serviço ou instalação
- Entidades responsáveis pela:
  - Operação do Sistema
  - Comercialização de Energia
  - Gestão de Recursos Setoriais

Destaque para os conceitos a seguir:



Incidente Cibernético

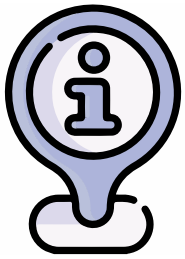
Invasão ou tentativa de invasão que possa colocar em risco a disponibilidade, integridade, confidencialidade ou autenticidade de sistemas de informações ou das informações de uma companhia

Incidente Cibernético de Maior Impacto

É definido de acordo com a classificação de severidade estabelecida pela companhia

Rede de Informação

Rede corporativa de dados da companhia, composta por toda infraestrutura própria e de terceiros



Informações Críticas

São aquelas com potencial de impacto negativo na prestação de serviços à população

Os pilares da segurança cibernética têm como objetivo proteger **confidencialidade**, **integridade** e **disponibilidade** de seus sistemas de informação. Esses três elementos são chamados de CID. As normas, políticas de segurança e o procedimento de segurança da informação devem estar alinhados com os objetivos de negócios, sendo que a mera tentativa de exploração de vulnerabilidade será considerada incidente cibernético.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Confidencialidade: as informações devem estar protegidas daqueles que não devam ou não precisem ter acesso a elas. Para garantir a confidencialidade, o agente deve adotar métodos de controle de acessos, como dupla autenticação, uso de senhas fortes, trocas frequentes de senhas, uso de criptografia, entre outros;

Integridade: refere-se à proteção das informações para que elas permaneçam confiáveis. Para garantir integridade, o agente deve criar mecanismos de controle que impeçam a alteração não autorizada ou indesejada dos dados;

Disponibilidade: as informações devem estar acessíveis àqueles com permissão para acessá-las. Para garantir a integridade, o agente deve investir na estabilidade de seus sistemas e eliminar eventuais vulnerabilidades.

Diretrizes para a Segurança Cibernética

- Adotar padrões e boas práticas em segurança cibernética (ex.: Normas ISO)
- Atuar com responsabilidade, zelo e transparência
- Promover e conscientizar sobre a cultura de segurança cibernética
- Utilizar as redes e os serviços de energia elétrica de forma segura
- Identificar, proteger, diagnosticar, responder e se recuperar de incidentes cibernéticos
- Identificar, avaliar, classificar e tratar riscos cibernéticos na estrutura estabelecida pelo agente
- Buscar cooperação entre os diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos, respeitadas as regras de confidencialidade das informações definidas pelo agente

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

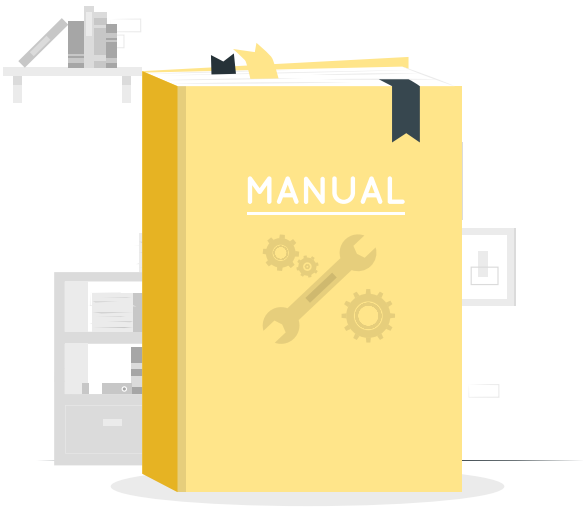
Conteúdo mínimo das Políticas de Segurança Cibernética no Setor Elétrico

De acordo com a Resolução Normativa ANEEL nº 964, as políticas de segurança cibernética devem contemplar, no mínimo:

- Objetivos de segurança cibernética e sua capacidade para prevenir, detectar, responder e reduzir a vulnerabilidade [do agente do setor] a incidentes cibernéticos;
- Classificação dos dados e das informações quanto à relevância;
- Procedimentos e controles de redução de vulnerabilidade [do agente do setor] a incidentes e de atendimento aos demais objetivos da segurança cibernética;
- Definição dos parâmetros para avaliar relevância dos incidentes cibernéticos;
- Definição de procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros, que manuseiem dados ou informações críticas, ou sejam relevantes para a condução das atividades operacionais em níveis equiparados ao do próprio agente;
- Definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes cibernéticos.

a) Medidas

- **Aplicação anual de pelo menos um modelo de maturidade** em segurança cibernética na companhia;
- **Medidas técnicas** que busquem garantir a segurança das informações críticas, incluindo as de rastreabilidade das informações;



OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

- **Registro, análise da causa e controle dos efeitos** de incidentes de maior impacto, abrangendo informações recebidas de empresas prestadoras de serviços a terceiros;

- **Mecanismos para prevenir, mitigar e recuperar** incidentes cibernéticos em sua rede de informação ou na rede das instalações, bem como para impedir que os incidentes afetem a operação; e

- **Procedimentos para prevenção, tratamento e resposta** a incidentes cibernéticos.

b) Treinamento e Conscientização

- Implementação de **programas de capacitação e de avaliação periódica de pessoal**;

- Plano de ação com medidas para **conscientização e educação** de seus usuários sobre aspectos de segurança cibernética;

- **Comprometimento da alta administração** com a melhoria contínua dos procedimentos; e

- **Simulações de cenários e ameaças** para testes de resiliência, de análise das ferramentas e da capacidade e tempo de resposta.

A Política de Segurança Cibernética deve ainda:

Ser **compatível com a relevância da instalação** no contexto do SIN (Sistema Interligado Nacional), bem como com a natureza e a complexidade de serviços, atividades, processos e sistemas;

Ser **compatível com a sensibilidade dos dados** e das informações sob sua responsabilidade;

Ser **disseminada aos profissionais e colaboradores das áreas**, em seus diversos níveis, papéis e responsabilidades, resguardando-se o compartilhamento de informações críticas apenas para pessoas que exerçam diretamente atividades de planejamento e execução da política;

Estabelecer **responsabilidades pela aplicação da política**, com identificação de pessoas e áreas competentes, bem como ponto focal para contato em eventuais urgências;

Designar dirigente responsável pela política de segurança cibernética, que pode desempenhar outras funções, desde que não haja conflito de interesses;

Ser aprovada pelo Conselho de Administração ou órgão de deliberação colegiado equivalente;

Ser revisada e atualizada periodicamente ou sempre que necessário; e

Estar disponível à ANEEL sempre que solicitada, juntamente com documentos complementares e comprovantes de sua aprovação interna pelo órgão competente.

Sobre Incidentes Cibernéticos

Qual incidente?

- De maior impacto
- Que afete substancialmente:
  - segurança das instalações;
  - operação;
  - serviços aos usuários; ou
  - segurança de dados.

O que fazer?

- Notificar equipe de coordenação setorial designada aos incidentes de maior impacto.
- A notificação deve incluir:
  - análise da **causa**;
  - análise de **impacto**;
  - ações de **mitigação**.

Quando?

- Assim que o agente tiver ciência do incidente ou de sua dimensão.

ATENÇÃO - A notificação não exclui o atendimento de outras obrigações previstas em leis.

Compartilhamento de Informações (cooperação)

Os agentes devem 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. Esse compartilhamento não pode ser restrito às empresas do mesmo grupo societário nem compreende as informações **classificadas como críticas** ou que possam comprometer a segurança de quem as comunica.

***Security by Design and Default*:**

A Resolução estabelece aos agentes do setor elétrico que procedimentos e controles devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas em suas atividades.

Determina, ainda, o **comprometimento da alta administração** com a melhoria contínua dos procedimentos relacionados à segurança cibernética.

OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Quais são os próximos passos?

Para atender às disposições da Resolução Normativa nº 964/2021, será necessário criar ou revisar:

1. **Política de Segurança da Informação**, que deverá prever conteúdo mínimo e diretrizes definidos na Resolução, contemplando, ainda, as Políticas de BYOD; de Uso de Dispositivos Móveis; de Backup; de Controle de Acesso; e de Uso de Controles Criptográficos;
2. Procedimento de **Classificação da Informação**;
3. Plano de **Resposta a Incidentes**;
4. Plano de **Recuperação de Desastres**; e
5. Plano de **Continuidade de Negócios**.

www.opiceblum.com.br
Al. Joaquim Eugênio de Lima, 680, 1º andar, Jardim Paulista, CEP: 01403-000, São Paulo - SP, Telefone: +55 (11) 2189-0061

@opiceblum