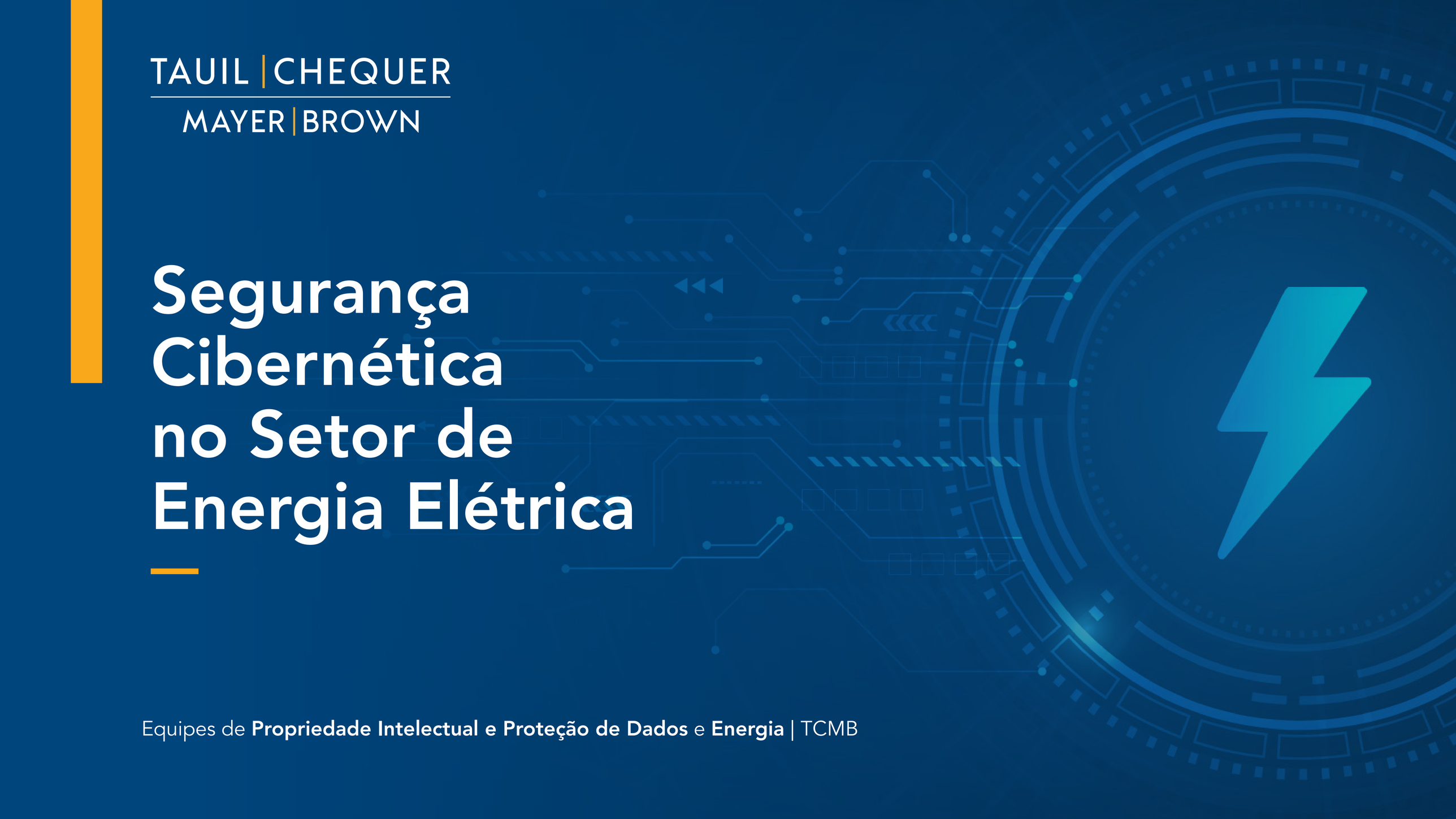
TAUIL | CHEQUER
MAYER | BROWN

Segurança Cibernética no Setor de Energia Elétrica



Equipes de **Propriedade Intelectual e Proteção de Dados** e **Energia** | TCMB

TAUIL | CHEQUER
MAYER | BROWN

Após um amplo debate com a sociedade, no âmbito da Consulta Pública n.º 007/2021, a Agência Nacional de Energia Elétrica (ANEEL) emitiu a Resolução Normativa nº 964, que apresenta os pilares para uma estrutura de segurança da informação no setor elétrico. As novas regras entraram em vigor em 1º de julho de 2022. É importante ressaltar que essa resolução não inibe o cumprimento integral da Lei Federal n.º 13.709/2018 (LGPD), que é aplicável a todos os agentes, independentemente do setor.

TAUIL | CHEQUER
MAYER | BROWN

ESCOPO E OBJETIVO

A resolução estabelece as diretrizes e o conteúdo mínimo das Políticas de Segurança Cibernética dos agentes do setor de energia elétrica e obriga os agentes a adotarem mecanismos de segurança da informação, de acordo com os requisitos elencados na norma, assim como obriga esses agentes a notificarem incidentes cibernéticos à ANEEL.

TAUIL | CHEQUER
MAYER | BROWN

A QUEM SE APLICA

Concessionários e permissionários de transmissão, geração e distribuição.

Autorizadas de instalações, como produtores independentes e autoprodutores.

Autorizados de serviço, tais como comercializadoras.

Entidades responsáveis pela operação do sistema, comercialização de energia e/ou gestão de recursos setoriais, tais como o ONS, a CCEE e a recém-criada Empresa Brasileira de Participações em Energia Nuclear e Binacional S.A. (ENBPar).

TAUIL | CHEQUER
MAYER | BROWN

NA TEORIA

A Resolução traz algumas definições relevantes para a compreensão:

INCIDENTE CIBERNÉTICO
Ocorrência que comprometa ou possa comprometer a disponibilidade, integridade, confidencialidade ou autenticidade de sistemas de informações ou das informações de uma companhia.

INCIDENTE CIBERNÉTICO DE MAIOR IMPACTO
Definido de acordo com a classificação de severidade estabelecida pela companhia.

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

REDE DE INFORMAÇÃO
rede corporativa de dados da companhia, composta por toda infraestrutura própria e de terceiros destinada aos ativos de tecnologia da informação.

TAUIL | CHEQUER
MAYER | BROWN

NA PRÁTICA

Política de Segurança Cibernética: deixou de ser apenas uma boa prática, para se tornar uma obrigação regulatória. Todas as empresas do setor devem estruturar uma Política de Segurança Cibernética, com os elementos mínimos abaixo, listados no artigo 4º.

- Prevenção, detecção, resposta e redução de vulnerabilidades a incidentes cibernéticos.
- Classificação de dados e informações quanto à relevância.
- Medidas técnicas, incluindo rastreabilidade para informações críticas.
- Registro, análise de causa e impacto e controle de efeitos de incidentes, inclusive quanto a informações recebidas de prestadores de serviços.
- Procedimentos para prevenção, tratamento e resposta a incidentes cibernéticos.

TAUIL | CHEQUER
MAYER | BROWN

NA PRÁTICA

Procedimentos e controles para a prevenção e tratamento de incidentes para prestadores de serviços e terceiros expostos a dados relevantes.

Parâmetros para a classificação de incidentes cibernéticos.

Mecanismo de disseminação de cultura de segurança cibernética, com programas de capacitação e avaliação periódica de pessoal; medidas de conscientização e educação de usuários; e comprometimento da administração com a melhoria contínua dos procedimentos de segurança cibernética.

Simulação de cenários e ameaças para testes de resiliência, bem como análise de ferramentas e capacidade e tempo de resposta.

Mecanismos de prevenção, mitigação e recuperação de incidentes na Rede de Informação ou na rede das instalações para impedir que afete a operação.

TAUIL | CHEQUER
MAYER | BROWN

NA PRÁTICA

Nível de profundidade da Política de Segurança Cibernética: deve ser aderente à relevância da instalação no contexto do Sistema Interligado Nacional (SIN), bem como à natureza e à complexidade dos serviços, atividades, processos e sistemas. Naturalmente, sistemas estruturalmente relevantes – como concessões de transmissão e distribuição – precisarão de uma maior atenção e detalhamento das suas políticas, mas é também necessário avaliar se um gerador – pelo simples fato de estar conectado ao SIN – pode causar impacto operacional.

Governança de Segurança Cibernética: o artigo 5° exige a definição de "papéis e responsabilidades" e demanda uma arquitetura de acessos apropriada para a criticidade da informação. Também é necessário estabelecer as responsabilidades internas na aplicação da política, indicando pessoas e áreas e pontos focais para casos urgentes. Está, ainda, prevista a designação de um diretor responsável pela Política de Segurança Cibernética, que poderá desempenhar outras funções, se não houver conflito de interesses.

TAUIL | CHEQUER
MAYER | BROWN

NA PRÁTICA

Alta Administração: a Política de Segurança Cibernética deverá ser aprovada pelo Conselho de Administração da empresa ou pelo órgão de deliberação colegiado equivalente e deverá ser atualizada periodicamente ou sempre que necessário.

Grupo Econômico: á possível estabelecer uma única política para empresas do mesmo grupo. Embora não esteja mencionado na normativa, recomendamos que, nesses casos, sejam também observadas as regras de compartilhamento de recursos humanos previstas na Resolução n.º 948/2021.

TAUIL | CHEQUER
MAYER | BROWN

NA PRÁTICA

Notificação de Incidentes: a resolução deixa claro que os agentes devem notificar à equipe de coordenação setorial[1], designada aos incidentes de segurança, apenas os incidentes de **maior impacto**, conforme definido internamente pelas companhias, ou os que **afetem substancialmente** a segurança das instalações, a operação, os serviços aos usuários ou a segurança de dados. A **notificação deve ser realizada assim que o agente tiver ciência do incidente e de sua dimensão**, sem prazo específico definido. Além da notificação à ANEEL, eventuais obrigações de notificação da Autoridade Nacional de Proteção de Dados, assim como dos titulares dos dados pessoais afetados pelo incidente, com base na LGPD, devem ser observadas pelos agentes.

Compartilhamento de Informações: a resolução estimula o compartilhamento de informações entre os agentes, não incluindo os realizados internamente em grupo societário.

[1] **Equipe de Coordenação Setorial**: o Governo Federal, por meio do Decreto n.º 10.748/2021, instituiu a Rede Federal de Gestão de Incidentes Cibernéticos, a qual define a equipe de coordenação setorial como a responsável pela prevenção, tratamento e resposta a incidentes cibernéticos das agências reguladoras e as obrigou a instituir essas equipes. Apesar de o decreto ter trazido a possibilidade de designação de uma instituição de fora do escopo da agência para atuar como a equipe de coordenação setorial, a referida hipótese não foi tratada na Análise de Impacto Regulatório no contexto da aprovação da Resolução n.º 964.

TAUIL | CHEQUER
MAYER | BROWN

PRÓXIMOS PASSOS

Com a entrada em vigor da Resolução n.º 964, a ANEEL já pode fiscalizar as empresas para verificar a existência da Política de Segurança Cibernética. Entre os documentos que podem ser solicitados estão:

- Política de Segurança Cibernética e documentos que comprovem a sua aprovação pelo órgão societário aplicável.
- Resultados dos modelos de maturidade.
- Riscos cibernéticos identificados e tratamento dado.
- Dados das equipes de prevenção, tratamento e resposta a incidentes cibernéticos.

Descumprir essa obrigação de envio de documentos ou informações solicitados pela ANEEL pode dar causa à aplicação de penalidade de multa, nos termos da Resolução n.º 846/2019.

TAUIL | CHEQUER
MAYER | BROWN

PARA ALÉM DA RESOLUÇÃO N.º 964

O **investimento em segurança da informação é primordial para setores críticos como o de energia**, reforçado inclusive pelo Decreto n.º 10.222/2020 que aprovou a Estratégia Nacional de Segurança Cibernética. Para além dos dados pessoais, eventuais ataques maliciosos aos sistemas informáticos de agentes estratégicos do setor energético podem levar à interrupção dos serviços, o que seria catastrófico sob diversos pontos de vista. Preocupar-se com a implementação de mecanismos técnicos e organizacionais que visem assegurar os seus sistemas deve ser encarado não apenas como uma obrigação regulatória, mas como um diferencial competitivo e reputacional, na medida em que cada vez mais diversos stakeholders têm exigido e até mesmo verificado níveis elevados de segurança da informação.

TAUIL | CHEQUER
MAYER | BROWN

CONTATOS

Débora Yanasse
dyanasse@mayerbrown.com
+55 21 2127 4276

Cristiane Manzueto
cmanzueto@mayerbrown.com
+ 55 21 2127 4235

TAUIL | CHEQUER

MAYER | BROWN