Relatório de descrição detalhada de procedimentos realizados para a avaliação dos Controles Gerais de Tecnologia da Informação relacionados ao CliqCCEE no período de julho a dezembro de 2024 dos Auditores Independentes

Câmara de Comercialização de Energia Elétrica (CCEE)

30 de janeiro de 2025

Building a better working world

São Paulo Corporate Towers
Av. Presidente Juscelino Kubitschek, 1.909
Vila Nova Conceição
04543-011 - São Paulo - SP - Brasil
Tel: +55 11 2573-3000
ey.com.br

Aos
Srs. administradores da Câmara de Comercialização de Energia Elétrica (CCEE)
São Paulo – SP

Prezados Senhores,

Em conformidade com os termos de Prestação de Serviços relativos à Asseguração Razoável, fomos contratados pela Câmara de Comercialização de Energia Elétrica (CCEE) com o objetivo de aplicar procedimentos que nos permitam concluir na forma de uma asseguração razoável sobre a implementação e operação dos objetivos de controles atrelados aos Controles Gerais de Tecnologia da Informação de Gestão de Acessos, Gestão de Mudanças e Gestão de Operações para o sistema CLIQCCEE descritos abaixo. Nossa avaliação é relativa ao segundo semestre de 2024, que compreende o período entre os dias 1 de julho de 2024 a 31 de dezembro de 2024.

Conforme previsto no tópico Opinião do ***Relatório de asseguração razoável dos auditores independentes sobre a avaliação dos Controles Gerais de Tecnologia da Informação relacionados ao CliqCCEE no período de julho a dezembro de 2024***, emitido em mesma data, elaboramos o seguinte documento com objetivo de detalhar os procedimentos realizados para avaliação de cada objetivo de controle, com base nos resumos de controles identificados.

Este documento foi preparado como complemento ao relatório de auditores independentes para uso exclusivo da CCEE, e não deve ser apresentado ou distribuído a terceiros, tendo em vista sua finalidade específica. Qualquer outra parte que obtiver acesso ao nosso documento, ou à cópia deste, e confiar nas informações nele contidas (ou ainda em qualquer parte dele) irá fazê-lo por própria conta e risco. Não aceitamos ou assumimos qualquer responsabilidade e negamos qualquer responsabilidade perante qualquer outra parte que não seja a CCEE pelo nosso trabalho, pelo documento apresentado, relatório de asseguração ou pelas nossas conclusões.

Com base nos procedimentos executados, não foram identificadas divergências materialmente relevantes em relação aos objetivos de controles dos Controles Gerais de Tecnologia da Informação relacionados ao CliqCCEE, conforme os critérios estabelecidos na sessão “Descrição dos Procedimentos Realizados” do Relatório de Asseguração Razoável dos Auditores Independentes. Nossa opinião pode ser observada no relatório citado.

São Paulo, 30 de janeiro de 2025.
Ernst & Young
Auditores Independentes S.S.
CNPJ 61.366.936/0001-25
CRC-SP-034519/O

HANALU RODRIGUES MARIANO:31232867896

Digitally signed by HANALU RODRIGUES MARIANO:31232867896
DN: cn=HANALU RODRIGUES MARIANO:31232867896, c=BR, o=ICP-Brasil, ou=VIDEOCONFERENCIA, email=HANALU.MARIANO@BR.EY.COM
Date: 2025.01.30 14:26:47 -03'00'

Hanalu Rodrigues Mariano
CRC-SP-350883/O
Diretora Executiva

São Paulo Corporate Towers
Av. Presidente Juscelino Kubitschek, 1.909
Vila Nova Conceição
04543-011 - São Paulo – SP - Brasil
Tel: +55 11 2573-3000
ey.com.br

Descrição dos controles considerados em cada objetivo de controle informado na seção "Descrição dos Procedimentos Realizados" do ***Relatório de asseguração razoável dos auditores independentes sobre a avaliação dos Controles Gerais de Tecnologia da Informação relacionados ao CliqCCEE no período de julho a dezembro de 2024***

- Objetivo de controle: Os controles devem prover segurança razoável de que apenas pessoas autorizadas tenham acesso aos dados, às aplicações, à configuração dos dispositivos de redes (incluindo programas, tabelas e recursos relacionados) e que elas possam apenas executar funções especificamente autorizadas.
    - Controles e procedimentos avaliados para esse objetivo de controle:

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de teste
Concessão de acessos A cada necessidade de novo acesso ao sistema CliqCCEE, deve ser aberto um chamado na ferramenta Jira informando usuário espelho ou permissões a serem atribuídas. Essa solicitação é submetida a um fluxo de aprovação, que é parametrizado por meio de regras definidas em banco de dados, pelo qual o Jira identifica o grupo aprovador necessário e considera os dados do Active Directory para determinar o usuário responsável. Após aprovação, a equipe da Gerência de Administração dos Agentes & Contratos (GAAC) é responsável pela concessão do acesso ao sistema CliqCCEE.	CLIQCCEE	Indagamos os responsáveis sobre os processos de solicitação, aprovação e concessão de acessos ao sistema CliqCCEE. Avaliamos, por meio de uma amostra de 5 itens, a existência de formalização da solicitação por meio de chamado na ferramenta. Inspecionamos que as aprovações ocorreram por pessoa devida e antes da concessão de acesso. Verificamos a documentação suporte sobre os acessos concedidos conforme solicitados.	Não foram identificadas exceções.
Revogação de acessos Quando há um desligamento, os responsáveis do RH são responsáveis por abrir um chamado na ferramenta JIRA. A partir disso, são criadas sub-tarefas para revogação dos acessos lógicos do colaborador. A equipe da Gerência de Administração dos Agentes & Contratos (GAAC) é responsável pela revogação no sistema CliqCCEE.	CLIQCCEE	Indagamos os responsáveis para inspeção do desenho de controle adotado pela companhia. Verificamos, por meio de uma amostra de 5 itens, que a revogação de acessos ocorre a partir da existência de formalização do desligamento via ferramenta de chamados. Inspecionamos que os acessos foram revogados e que os colaboradores não tiveram acesso na aplicação após seu desligamento.	Não foram identificadas exceções.

São Paulo Corporate Towers
Av. Presidente Juscelino Kubitschek, 1.909
Vila Nova Conceição
04543-011 - São Paulo – SP - Brasil
Tel: +55 11 2573-3000
ey.com.br

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de teste
Alteração de acessos O processo de alteração de acessos da aplicação é gerido via ferramenta de gestão de chamados Jira. Por meio dela, quando colaborador transferido tem alteração no cargo ou gerência, os acessos são submetidos a revisão e aprovação. O fluxo de aprovação é parametrizado por meio de regras definidas em banco de dados, pelo qual o Jira identifica o grupo aprovador necessário e considera os dados do Active Directory para determinar o usuário responsável. Após aprovações, a equipe da Gerência de Administração dos Agentes & Contratos (GAAC) realiza as alterações conforme aprovações, revogando acessos não mais necessários e concedendo os acessos coerentes com as novas atribuições.	CLIQCCEE	Indagamos os responsáveis para inspeção do desenho de controle adotado pela companhia. Verificamos, por meio de uma amostra de 5 itens, que a alteração do acesso é devidamente formalizada aos gestores para aprovação via chamado.	Não foram identificadas exceções.
Usuários privilegiados Os acessos privilegiados ao Active Directory são adequados, assegurando que apenas indivíduos com cargos e funções específicas possuam permissões elevadas na rede.	AD	Inspecionamos as contas de usuários com acesso privilegiado à rede da companhia com o objetivo de confirmar que apenas colaboradores autorizados possuem função administrativa.	Não foram identificadas exceções.
Usuários privilegiados Os acessos privilegiados ao banco de dados do sistema CliqCCEE são adequados, assegurando que apenas indivíduos com cargos e funções específicas possuam permissões elevadas.	Banco de Dados	Inspecionamos as contas de usuários com acesso privilegiado ao banco de dados que suporta o sistema CliqCCEE com o objetivo de confirmar que apenas colaboradores autorizados possuem função administrativa.	Não foram identificadas exceções.
Usuários privilegiados Os acessos privilegiados ao sistema CliqCCEE são adequados, assegurando que apenas indivíduos com cargos e funções específicas possuam permissões elevadas no sistema CliqCCEE.	CLIQCCEE	Inspecionamos as contas de usuários com acesso privilegiado ao sistema CliqCCEE com o objetivo de confirmar que apenas colaboradores autorizados possuem função administrativa no sistema.	Não foram identificadas exceções.
Parâmetros de Senha As senhas de acesso ao sistema CliqCCEE são parametrizadas de acordo com as boas práticas de mercado, exigindo quantidade de caracteres mínimos e complexidade.	CLIQCCEE	Inspecionamos as configurações de senha do sistema CliqCCEE com o objetivo de confirmar que os critérios adotados estavam configurados de acordo com as configurações mínimas de segurança.	Não foram identificadas exceções.
Parâmetros de Senha As senhas de acesso ao Active Directory são parametrizadas de acordo com as boas práticas de mercado, exigindo quantidade de caracteres mínimos e complexidade.	AD	Inspecionamos as configurações de senha do domínio de rede com o objetivo de confirmar que os critérios de complexidade de senha, tamanho, renovação, histórico de senhas e bloqueio por tentativas falhas estavam configurados de acordo com as políticas de segurança e senha definidas pela companhia.	Não foram identificadas exceções.
Parâmetros de Senha As senhas de acesso à ferramenta de chamados Jira são parametrizadas de acordo com as boas práticas de mercado, exigindo quantidade de caracteres mínimos e complexidade.	Jira	Inspecionamos que a ferramenta Jira possui tecnologia *single sign-on* com o domínio de rede. Ainda, com o objetivo de confirmar que os critérios de complexidade de senha, tamanho, renovação, histórico de senhas e bloqueio por tentativas falhas estavam configurados de acordo com as políticas de segurança e senha definidas pela companhia, verificamos os parâmetros do AD.	Não foram identificadas exceções.

São Paulo Corporate Towers
Av. Presidente Juscelino Kubitschek, 1.909
Vila Nova Conceição
04543-011 - São Paulo – SP - Brasil
Tel: +55 11 2573-3000
ey.com.br

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de teste
Parâmetros de Senha As senhas de acesso à ferramenta de automação de desenvolvimento de mudanças Jenkins são parametrizadas de acordo com as boas práticas de mercado, exigindo quantidade de caracteres mínimos e complexidade.	Jenkins	Inspecionamos que a ferramenta Jenkins possui tecnologia *single sign-on* com o domínio de rede. Ainda, com o objetivo de confirmar que os critérios de complexidade de senha, tamanho, renovação, histórico de senhas e bloqueio por tentativas falhas estavam configurados de acordo com as políticas de segurança e senha definidas pela companhia, verificamos os parâmetros do AD.	Não foram identificadas exceções.
Parâmetros de Senha As senhas de acesso à ferramenta de gerenciamento de backup de banco de dados SGAC são parametrizadas de acordo com as boas práticas de mercado, exigindo quantidade de caracteres mínimos e complexidade.	SGAC	Inspecionamos que a ferramenta SGAC possui tecnologia *single sign-on* com o domínio de rede. Ainda, com o objetivo de confirmar que os critérios de complexidade de senha, tamanho, renovação, histórico de senhas e bloqueio por tentativas falhas estavam configurados de acordo com as políticas de segurança e senha definidas pela companhia, verificamos os parâmetros do AD.	Não foram identificadas exceções.
Parâmetros de Senha As senhas de acesso ao banco de dados do sistema CliqCCEE são parametrizadas de acordo com as boas práticas de mercado, exigindo quantidade de caracteres mínimos e complexidade.	Banco de Dados	Inspecionamos as configurações de senha do banco de dados do sistema CliqCCEE com o objetivo de confirmar que os critérios de complexidade de senha, tamanho, renovação, histórico de senhas e bloqueio por tentativas falhas estavam configurados de acordo com as políticas de segurança e senha definidas pela companhia.	Não foram identificadas exceções.
Usuários privilegiados Os acessos privilegiados ao Jira são adequados, assegurando que apenas indivíduos com cargos e funções específicas possuam permissões elevadas na ferramenta de gerenciando de chamados.	Jira	Inspecionamos as contas de usuários com acesso privilegiado à ferramenta de chamados Jira com o objetivo de confirmar que apenas colaboradores autorizados possuem acesso a alterar as regras de fluxos de chamados.	Não foram identificadas exceções.
Usuários privilegiados Os acessos privilegiados ao Jenkins são adequados, assegurando que apenas indivíduos com cargos e funções específicas possuam permissões elevadas na ferramenta de automação de desenvolvimento de mudanças.	Jenkins	Inspecionamos as contas de usuários com acesso privilegiado à ferramenta Jenkins com o objetivo de confirmar que apenas colaboradores autorizados possuem acesso de gestão na ferramenta de automação de desenvolvimento de mudanças.	Não foram identificadas exceções.
Usuários privilegiados Os acessos privilegiados ao Veeam são adequados, assegurando que apenas indivíduos com cargos e funções específicas possuam permissões elevadas na ferramenta de gerenciando de backup do sistema CliqCCEE.	Veeam	Inspecionamos as contas de usuários com acesso privilegiado à ferramenta Veeam com o objetivo de confirmar que apenas colaboradores autorizados possuem acesso de gestão na ferramenta de monitoramento de rotinas automáticas de backup do sistema CliqCCEE.	Não foram identificadas exceções.
Usuários privilegiados Os acessos privilegiados ao SGAC são adequados, assegurando que apenas indivíduos com cargos e funções específicas possuam permissões elevadas na ferramenta de gerenciamento de backup de banco de dados.	SGAC	Inspecionamos as contas de usuários com acesso privilegiado à ferramenta SGAC com o objetivo de confirmar que apenas colaboradores autorizados possuem acesso de gestão na ferramenta de monitoramento de rotinas automáticas de backup do banco de dados do sistema CliqCCEE.	Não foram identificadas exceções.

São Paulo Corporate Towers
Av. Presidente Juscelino Kubitschek, 1.909
Vila Nova Conceição
04543-011 - São Paulo – SP - Brasil
Tel: +55 11 2573-3000
ey.com.br

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de teste
Controle a nível de entidade - Procedimentos Administrativos	-	Observamos a existência de um organograma que define as responsabilidades e atribuições de cada área, bem como estrutura da área de TI. Verificamos, por meio de uma amostra de 5 itens, a existência de processos de formação e treinamento dos funcionários para adoção e cumprimento das políticas e procedimentos de segurança da informação. Validamos, com bases nas amostras, a formalização de contratação conforme guia de ética e responsabilidade, proteção de dados e demais assuntos administrativos pertinentes. Avaliamos a existência de tratativa e monitoramento para incidentes referentes à segurança da informação.	Não foram identificadas exceções.
Data Center - Avaliação dos acessos físicos A CCEE possui um contrato com a Ascenty para utilização de data center, o qual possui acesso restrito. Para garantir a adequação desses acessos, quadrimestralmente é realizada a revisão dos colaboradores com acesso ao portal da Ascenty pela equipe de Infraestrutura & Tecnologia (GITC). Esses colaboradores possuem permissão para acesso físico.	-	Verificamos a existência de revisão dos usuários com acesso ao ambiente físico em que estão hospedados os servidores do sistema CliqCCEE.	Não foram identificadas exceções.

- Objetivo de controle: Os controles devem prover segurança razoável de que apenas mudanças autorizadas, testadas e aprovadas sejam executadas nas aplicações, interfaces e banco de dados que suportem as aplicações relevantes e os controles dependentes de TI relevantes para os processos.
    - Controles e procedimentos avaliados para esse objetivo de controle:

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de teste
Segregação de Ambientes Os ambientes de desenvolvimento, homologação e produção do sistema CliqCCEE são segregados.	CLIQCCEE	Validamos que os ambientes de desenvolvimento, homologação e produção são segregados.	Não foram identificadas exceções.
Segregação de Funções Os acessos aos ambientes de desenvolvimento e produção são segregados de acordo com as funções.	CLIQCCEE	Inspecionamos os usuários com acesso a implementar mudanças com objetivo de verificamos que somente colaboradores autorizados possuem esse acesso. Verificamos que a existência de restrição de usuários responsáveis por desenvolvimento ao ambiente produtivo.	Não foram identificadas exceções.

São Paulo Corporate Towers
Av. Presidente Juscelino Kubitschek, 1.909
Vila Nova Conceição
04543-011 - São Paulo – SP - Brasil
Tel: +55 11 2573-3000
ey.com.br

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de teste
Mudanças Normais, Emergênciais e Patches A cada necessidade de mudança que impacte o funcionamento o banco de dados, é aberto um chamado na ferramenta Jira indicando as necessidades a serem atendidas. Essas são testadas e aprovadas por pessoas devidas. O fluxo de aprovação é parametrizado por meio de regras definidas em banco de dados, pelo qual o Jira identifica o grupo aprovador necessário e considera os dados do Active Directory para determinar o usuário responsável. Ao fim desse fluxo, a mudança é devidamente implementada e o chamado é encerrado.	Banco de Dados	Indagamos os responsáveis para inspeção do desenho de controle adotado pela companhia. Observamos, junto a companhia, que apenas 1 mudança em banco de dados ocorreu dentro do período avaliado. Inspecionamos a abertura de solicitação via ferramenta de chamados para que seja realizada a mudança no banco de dados. Verificamos que há aprovação antes da implementação da mudança.	Não foram identificadas exceções.
Mudanças Normais, Emergênciais e Programadas A cada necessidade de mudança, é aberto um chamado na ferramenta Jira indicando as necessidades a serem atendidas. Essas são testadas e aprovadas por pessoas devidas. O fluxo de aprovação é parametrizado por meio de regras definidas em banco de dados, pelo qual o Jira identifica o grupo aprovador necessário e considera os dados do Active Directory para determinar o usuário responsável. Ao fim desse fluxo, a mudança é devidamente implementada e o chamado é encerrado.	CLIQCCEE	Indagamos os responsáveis para inspeção do desenho de controle adotado pela companhia. Inspecionamos, por meio de uma amostra de 11 itens, a abertura de solicitação via ferramenta de chamados para que seja realizada a mudança no sistema CliqCCEE. Validamos, por meio das amostras selecionadas, a existência de testes da mudança desenvolvida. Verificamos que há aprovação antes da implementação da mudança.	Não foram identificadas exceções.

- Objetivo de controle: Os controles devem prover segurança razoável de que incidentes e problemas na infraestrutura e na execução das aplicações sejam identificados, monitorados, investigados e resolvidos tempestivamente.
    - Controles e procedimentos avaliados para esse objetivo de controle:

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de teste
Monitoramento de Rotinas Automáticas As rotinas de backup de banco de dados são monitoradas pela ferramenta SGAC, que identifica ocorrências de falha na execução e notifica a equipe responsável diretamente via e-mails diários. Para o caso de rotinas que tenham reexecutado com sucesso automaticamente após a falha, não se faz necessário a abertura de um chamado para tratativa.	Banco de dados	Inspecionamos a utilização da ferramenta de monitoramento da rotina automática de backup. Por meio da amostra de 3 meses, validamos que a situação das execuções é notificada (sucesso ou erro) e verificamos que, em caso de erro, a rotina é reexecutada. Não houve ocorrência, em nossa amostra, de casos em que a reexecução automática tenha resultado em outro erro. Desse modo, esse aspecto não foi avaliado.	Não foram identificadas exceções.

São Paulo Corporate Towers
Av. Presidente Juscelino Kubitschek, 1.909
Vila Nova Conceição
04543-011 - São Paulo – SP - Brasil
Tel: +55 11 2573-3000
ey.com.br

Controle	Ambiente	Procedimentos realizados pela EY	Resultados de Teste
Monitoramento de Rotinas Automáticas As rotinas de backup do sistema CliqCCEE são monitoradas pela ferramenta Veeam, que identifica ocorrências de falha na execução e notifica a equipe responsável diretamente via e-mails diários. Para o caso de rotinas que tenham reexecutado com sucesso automaticamente após a falha, não se faz necessário a abertura de um chamado para tratativa.	CLIQCCEE	Inspecionamos a utilização da ferramenta de monitoramento da rotina automática de backup. Verificamos os schedules dos jobs de backup diário e mensal. Por meio da amostra de 3 execuções mensais e 10 execuções diárias, validamos que a situação sas execuções é notificada e verificamos que, em caso de erro, a rotina é reexecutada. Não houve ocorrência, em nossa amostra, de casos em que a reexecução automática tenha resultado em outro erro. Desse modo, esse aspecto não foi avaliado.	Não foram identificadas exceções.
Backup A ferramenta Veeam está parametrizada de modo a realizar backups diários e mensais dos dados do sistema CliqCCEE.	CLIQCCEE	Inspecionamos os schedules de backup. Validamos os usuários com permissão de alteração dessas parametrizações.	Não foram identificadas exceções.
Workflow de aprovações de chamados - Ferramenta Jira Todos os chamados criados no Jira, sejam referentes a acessos ou mudanças, são direcionados a aprovação de acordo com regras previamente parametrizadas.	Jira Banco de dados x Jira Jira x AD	Observamos a utilização da ferramenta Jira para gerenciamento de chamados, inspecionamos o fluxo de automatização da ferramenta e verificamos o motor de regras definido no banco de dados para direcionamento de aprovação (conforme comunicação com AD).	Não foram identificadas exceções.