PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Treinamento Recomendado: ☒ - formal ☐ - leitura (sem necessidade de manter em registro)

Controle de Revisão

Revisão	Data	Item	Descrição das Alterações

O DOCUMENTO ORIGINAL ASSINADO ENCONTRA-SE ARQUIVADO NO CCBE.

ESTE DOCUMENTO UMA VEZ IMPRESSO SERÁ CONSIDERADO CÓPIA NÃO CONTROLADA

Elaborado por: Tânia de A. D. de Britto Pereira Coordenadora Administrativo/Financeiro	**Visto**	**Verificado por:**	**Visto** 08/09/2023
Verificado por: Walter Luiz Alves de Oliveira Junior Gerente de Consórcio	**Visto**	Walter Alves	**Data:** 08/09/2023
Aprovado por: Walter Luiz Alves de Oliveira Junior Gerente de Consórcio	**Visto**	Walter Alves	**Data:** 08/09/2023
Aprovado por: Guilherme Bretas Nunes de Lima Diretor Presidente	**Visto**	Guilherme Bretas Nunes de Lima	**Data:** 08/09/2023
Aprovado por: Sandro Magno de Figueiredo e Horta Diretor de Operação	**Visto**		**Data:** 08/09/2023

SUMÁRIO

1. INTRODUÇÃO 3
2. OBJETIVOS 3
3. APLICAÇÕES 3
4. PRINCÍPIOS 4
5. PROTEÇÃO DE DADOS 4
6. REQUISITOS 5
7. RESPONSABILIDADES DOS COLABORADORES 5
8. RESPONSABILIDADES DOS GESTORES ..... **Erro! Indicador não definido.**
9. USO DE CORREIO ELETRÔNICO 6
10. USO DA INTERNET 7
11. IDENTIFICAÇÃO ..... **Erro! Indicador não definido.**
12. USO DE COMPUTADORES E RECURSOS TECNOLÓGICOS 8
13. REGRAS NO USO DE COMPUTADORES E EQUIPAMENTOS DE INFORMÁTICA 9
14. DISPOSITIVOS MÓVEIS DE COMUNICAÇÃO 9
15. BACKUPS 10
16. HOME OFFICE 10
17. AUDITORIAS 12
18. DISPOSIÇÕES FINAIS 12

1 - INTRODUÇÃO

Esta Política de Segurança da Informação, também referida como PSI, é um documento que visa orientar e estabelecer as diretrizes corporativas para a proteção dos ativos de informação, garantir a integridade, disponibilidade e prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição e ser apresentada a todos os usuários de tecnologia com a coleta de sua assinatura como termo de aceite das normas. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão e segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

2 - OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores, prestadores de serviço e visitantes seguirem padrões de comportamento relacionados à segurança da informação adequadas às necessidades de negócio e de proteção da empresa e do indivíduo. Definir normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento levando em consideração os seguintes requisitos:

Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la na guarda ou transmissão, contra alterações indevidas intencionais ou acidentais;

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3 - APLICAÇÕES DA PSI

Todas as diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, prestadores de serviços e visitantes, e se aplicam a acesso à informação em qualquer meio ou suporte, e uso de equipamentos, devendo dar ciência a cada usuário de que os ambientes, sistemas, meios de comunicação, computadores e redes da empresa poderão ser monitorados e gravados, sendo esta PSI a prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada usuário se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu

gestor ou do departamento de TI sempre que não tiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4 - PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos usuários como resultado da atividade profissional contratada pela empresa, pertence à instituição, devendo as exceções serem explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é proibido, visando não prejudicar o desempenho dos sistemas, segurança, e integridade das informações.

A empresa, por meio de ferramentas adequadas, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade, integridade e segurança das informações utilizadas.

5 - PROTEÇÃO DE DADOS

A segurança da informação sempre foi de extrema importância para a empresa, ela diz respeito à proteção dos dados, com a intenção de preservar seus respectivos valores para a organização e o indivíduo.

Garantir a segurança da informação exige atenção e conscientização por parte de todos. Os dados que coletamos para fins de uso da internet e intranet podem compreender: nome, sobrenome, data de nascimento, login, senha e endereço de IP (“internet protocol”). A finalidade da coleta de cada dado é:

a) Armazenamos nome e sobrenome para fins de cadastro do usuário;
b) Armazenamos data de nascimento dos sócios e funcionários para elaborar a lista de aniversariantes, a qual é coletada através da Ficha de Registro Funcional;
c) Armazenamos login porque é o cadastro no sistema – e em regra é o endereço de e-mail do funcionário;
d) Armazenamos senha de forma segura, protegida por criptografia e, portanto, impossibilitando que um funcionário ou terceiro conheçam a senha de outro funcionário;

e) Armazenamos o IP da máquina para fins de segurança da empresa, especialmente para saber de onde o sistema está sendo acessado pelo colaborador.

Prazo de tratamento e guarda desses dados: realizamos a guarda dos dados referidos neste item durante o período de vigência do contrato de trabalho ou da prestação de serviços, não atingindo os dados pessoais de contrato de trabalho e de prestação de serviços coletados para finalidades diversas, os quais incidirão outros prazos de retenção.

6 - REQUISITOS DA PSI

Para uniformidade da informação, a PSI deverá ser comunicada a todos os usuários já existentes e aos novos usuários assim que tenham o primeiro contato com os sistemas da empresa, para que a política seja cumprida dentro e fora da empresa. Tanto a PSI quanto às normas, deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada.

A responsabilidade em relação a segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos, devendo estes assinar o termo de responsabilidade que será arquivado junto ao departamento de TI.

Todo incidente que afete a segurança da informação deverá ser comunicado com urgência ao departamento de TI para que este defina a melhor ação a ser tomada. Ferramentas apropriadas serão utilizadas para registrar atividades em todos os desktops, notebooks, dispositivos móveis, acessos à internet, correio eletrônico, equipamentos e sistemas de comunicação em geral para reduzir os riscos.

A organização exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento dos requisitos nesta PSI acarretará violação às regras internas da organização e sujeitará o usuário às medidas administrativas e legais cabíveis.

7 - RESPONSABILIDADES DOS COLABORADORES

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da organização.
Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a organização ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

8 - RESPONSABILIDADES DOS GESTORES

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da política, exigindo a assinatura do Termo de compromisso, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informação da organização.

9 - USO DE CORREIO ELETRÔNICO

O uso do correio eletrônico é para fins corporativos e relacionados às atividades do colaborador usuário dentro da organização. A utilização desse serviço para fins pessoais é permitida, desde que feita com bom senso, e não ponha em risco a organização e não cause impacto no tráfego da rede. Acrescentamos que é terminantemente proibido o uso do correio eletrônico para:

- mensagens não solicitadas para múltiplos destinatários, ou que contenham qualquer ato, ou forneça orientação que conflite ou contrarie os interesses da organização, contenha ameaças eletrônicas, contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, . inf) ou qualquer outra extensão que represente um risco a segurança.;
- mensagens que tenham conteúdo considerado impróprio, obsceno ou ilegal, de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, ou que contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- mensagens com conteúdo multimídia, ou links que direcionam a outros sites que possam conter este tipo de conteúdo ou que ponham em risco a segurança da informação, e ainda mensagens com anexos superiores a 10 Mb.
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem prévia autorização, enviar material protegido por direitos autorais sem a permissão do detentor dos direitos.

10 - USO DE INTERNET

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a monitoramento e divulgação. Portanto, a organização em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a internet.

Os equipamentos, links, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da organização, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, em nuvem, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A organização, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividade ilícita poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a organização cooperar ativamente com as autoridades competentes.

O uso de sites de notícias, serviços, buscas, é aceitável, desde que não comprometa o tráfego de rede, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesses com seus objetivos de negócio, ficando proibido a divulgação e/ou o compartilhamento indevido de informações da área administrativa em lista de discussões, sites ou redes sociais, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Fica proibido todo o processo de download e upload, bem como distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. O uso, instalação, cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software ou mídia não autorizada baixada e armazenada, será excluída pelo departamento de TI.

Como regra geral, músicas, vídeos, jogos, material de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Os colaboradores não poderão utilizar recursos da organização para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Acesso a software de compartilhamento, serviços de streaming, não serão permitidos, já serviços de comunicação instantânea serão disponibilizados aos

usuários que necessitarem desta ferramenta para facilitar o contato com outros centros de negócio, clientes ou fornecedores.

11 - IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a organização sendo que o uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Todo dispositivo de identificação, como nome de usuário e crachás, não poderá ser compartilhado com outras pessoas em nenhuma hipótese, caso haja a necessidade deste procedimento, o gestor deverá informar por escrito, ou por e-mail quais serão as pessoas responsáveis por este login.
Todas as senhas deverão ter um tamanho mínimo de 8 caracteres sendo obrigado o uso de pelo menos três tipos de caracteres diferentes, sendo eles, letras maiúsculas, minúsculas, números ou caracteres especiais, estas senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos, não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento, e não devem ser constituídas de combinações óbvias de teclado, como abcdefg, 876543, entre outras.

A periodicidade máxima para troca de senha é de 60 (Sessenta) dias, não podendo ser repetidas as 3 (três) últimas senhas.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao departamento de TI, a fim de que essa providência seja tomada.
Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente ao departamento de TI para cadastrar uma nova.

12 - USO DE COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da organização, ficando proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do departamento de TI. Casos de novas aquisições deverão ser encaminhadas com antecedência, para que se tenha tempo hábil de orçamento, compra e configuração.

Atualizações e correções de segurança em sistema operacional, antivírus ou aplicativos, somente serão aplicadas pelo departamento de TI, que garantirá as versões mais atuais instaladas nas estações de trabalho.
O usuário, em caso de suspeita de vírus ou problema na funcionalidade, deverá acionar imediatamente o departamento de TI.

Arquivos pessoais, e/ou não pertinentes ao negócio (fotos, músicas, vídeos etc.) não deverão ser copiados/armazenados nas estações de trabalho e muito menos para drives de rede, pois podem sobrecarregar o armazenamento. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente até mesmo sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores, deverão ser salvos em drives de rede ou na nuvem. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

13 - REGRAS NO USO DE COMPUTADORES E EQUIPAMENTOS DE INFORMÁTICA

- Não usar qualquer dispositivo estranho conectado ao computador, como pen-drive, celulares.

- Não consumir comidas ou bebidas na mesa de trabalho e próximo aos equipamentos.

- Não abrir ou movimentar o equipamento para mudança de local ou manutenção sem o prévio conhecimento da área de TI - Sempre manter o equipamento protegido por senha quando o usuário for se ausentar.

14 - DISPOSITIVOS MÓVEIS DE COMUNICAÇÃO

Quando se descreve um dispositivo móvel, entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da organização, tais como: Tablets, smartphones e pendrives.

A organização, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador deverá realizar periodicamente cópia de segurança dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos, devendo ainda utilizar senhas de bloqueio automático para seu dispositivo móvel.

É de responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel de propriedade da organização, notificar imediatamente seu gestor direto e o departamento de TI, e procurar ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O uso indevido do dispositivo móvel caracteriza o ato de assumir todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, ou custo extra que venha causar à organização.

15 - BACKUPS

Backups dos servidores serão efetuados de forma automatizada com agendamento para serem executados fora do horário comercial, quando houver nenhuma ou pouca utilização de acessos e processos, sendo armazenado em nuvem.

16 - HOME OFFICE

A realização de trabalho remoto pelo colaborador não afasta seus deveres e obrigações dispostos neste instrumento e qualquer outro documento que vincule o colaborador e o Consórcio Capim Branco Energia, sendo o dever de sigilo, segurança, inviolabilidade e zelo, vinculados de igual forma para equipamentos particulares do colaborador, ambientes fora das dependências do Consórcio Capim Branco Energia e redes que não integrem a rede corporativa CCBE, desde que contenham, tratem ou envolvam todo e qualquer sistema e informação do Consórcio Capim Branco Energia ou que por ele tenham sido disponibilizados.

As informações disponibilizadas pelo CCBE deverão ser tratadas somente nos dispositivos eletrônicos e em rede particular do CCBE, sendo expressamente vedado o tratamento em equipamentos e redes alheias à prestação dos serviços. Para a realização de trabalho remoto o colaborador terá acesso às informações estritamente necessárias para a sua correta prestação.

O colaborador deverá conter em seu computador e rede pessoal senha considerada segura e complexa para acesso. Da mesma forma, o colaborador deve evitar a utilização de datas de aniversário e algarismos sequenciais para a elaboração de senhas.

O dispositivo eletrônico utilizado em trabalho remoto deverá ser automaticamente bloqueado após, no máximo, 05:00 (cinco) minutos de inatividade.
Em havendo a utilização de documentos físicos, o colaborador deverá ter o mesmo zelo, não o tornando acessível a terceiros estranhos ao respectivo serviço. A perda de registros em papel, qualquer que seja a natureza do seu

conteúdo, será considerada uma violação de privacidade de dados e deverá ser comunicada imediatamente ao Consórcio Capim Branco Energia.

Quando o trabalho remoto for realizado pelo colaborador em local público, este deverá reforçar os cuidados com as informações do CCBE, não podendo, por exemplo, deixar o meio eletrônico aberto e desbloqueado sem a sua presença. De igual forma, é vedado o acesso à rede de internet pública ou que não possua elevados requisitos de segurança.

É vedada a utilização de dispositivos eletrônicos do Consórcio Capim Branco Energia para questões pessoais do colaborador. Caso seja observado o uso dos dispositivos do CCBE para questões pessoais do colaborador, aquele se reserva o direito de efetuar cobrança por eventuais custos gerados.

Havendo a perda ou o roubo do equipamento eletrônico utilizado para o trabalho remoto ou que contenha informações do Consórcio Capim Branco Energia; bem como tenha sido o dispositivo eletrônico acessado por hacker, vírus, malware, entre outros que possam ocasionar o vazamento de dados, o colaborador deverá comunicar imediatamente o CCBE, a partir da sua ciência do fato para que esta proceda com os devidos cuidados e alterações necessárias de códigos e sistemas internos. Havendo demora na comunicação ao Consórcio Capim Branco Energia, o colaborador será diretamente responsável pelas perdas e danos a que der causa.

Nos dispositivos eletrônicos que contenham documentos e informações do Consórcio Capim Branco Energia, o colaborador se compromete a realizar download de aplicativos nas lojas oficiais de app, sendo, no caso dos sistemas operacionais Android e iOS, Google Play e App Store, respectivamente, evitando o download de aplicativos maliciosos, os quais poderão vir a comprometer os dados do Consórcio Capim Branco Energia.

É dever do colaborador realizar a atualização dos sistemas operacionais dos respectivos dispositivos eletrônicos, do software de antivírus e quaisquer outros sistemas que garantem a segurança das informações do CCBE. A sua não atualização poderá deixar os dispositivos vulneráveis e expostos a ataques externos.

É vedado ao colaborador salvar documentos e informações do Consórcio Capim Branco Energia e dos respectivos serviços que o colaborador estiver prestando ao CCBE em pendrives, mp3 ou qualquer outro dispositivo portátil, bem como transferi-los a contas de e-mail pessoais e salvá-los em meio eletrônico próprio.

O manejo dos documentos e informações do Consórcio Capim Branco Energia utilizados na prestação dos serviços deverá ocorrer na rede do CCBE. Caso seja estritamente necessário o download de documentos do CCBE do sistema próprio do CCBE, o documento deverá ser salvo em sistema de nuvem.

Os deveres e obrigações aqui dispostos sobre home office se vinculam a dispositivos eletrônicos como desktop, notebook, tablet, smartphone, celular, telefone fixo, dentre outros dispositivos que tiverem acesso às informações e documentos do CCBE.

A violação dos deveres e obrigações aqui dispostos ocasionará ao colaborador responsabilidade pelas perdas e danos a que der causa.

17 - AUDITORIAS

Todos os colaboradores que utilizem a rede corporativa (informática e telefonia) poderão ser submetidos à auditoria, realizada por um profissional da administração da rede, área de TI do Consórcio Capim Branco Energia ou empresa especializada, com objetivo de verificar o cumprimento das normas estabelecidas.

A auditoria poderá será realizada semanalmente em computadores ou notebooks escolhidos aleatoriamente e, verificada alguma não-conformidade, será instaurada uma sindicância interna voltada à apuração de responsabilidades e classificação da gravidade da violação das normas de utilização aqui elencadas.

Após a classificação da gravidade, a não-conformidade será comunicada aos setores competentes para adoção das providências cabíveis.

A auditoria tem como objetivos não só a verificação do cumprimento de deveres por parte do colaborador, mas também a verificação do ambiente visando melhorias de projeto e segurança. Desta forma, o colaborador jamais poderá se negar a fornecer informações solicitadas pelo Consórcio Capim Branco Energia.

18 - DISPOSIÇÕES FINAIS

Tal como a ética, o comprometimento e a segurança devem ser entendidos como parte fundamental para um bom funcionamento e garantia de continuidade dos processos. Qualquer incidente de segurança, deverá e será tratado com extrema rigidez para que se busque uma solução rápida e eficiente.

Cargo	CCBE-PO-DE-05-Politica de Segurança da informação
Nome de arquivo	CCBE-PO-DE-05-Pol..._versão final.pdf
Identificação do documento	4cc416c8a25b5dc36a4fbfed60932e9e6aa79ca2
Formato de data da trilha de auditoria	DD / MM / YYYY
Status	● Assinados

Histórico do documento

ENVIADO

12 / 12 / 2023
10:05:29 UTC-3

Enviadas para assinatura de Tânia de Araujo Duprat de Britto Pereira (tania@ccbe.com.br), Walter Luiz Alves de Oliveira Junior (walter.alves@ccbe.com.br), Guilherme Bretas Nunes de Lima (guilherme.lima@aliancaenergia.com.br) and Sandro Magno de Figueiredo e Horta (sandro.horta@aliancaenergia.com.br) por adminhellosign@ccbe.com.br
IP: 189.37.64.68

VISUALIZADO

12 / 12 / 2023
10:08:40 UTC-3

Visualizado por Sandro Magno de Figueiredo e Horta (sandro.horta@aliancaenergia.com.br)
IP: 179.220.159.235

VISUALIZADO

12 / 12 / 2023
10:16:19 UTC-3

Visualizado por Tânia de Araujo Duprat de Britto Pereira (tania@ccbe.com.br)
IP: 189.37.64.68

Cargo	CCBE-PO-DE-05-Politica de Segurança da informação
Nome de arquivo	CCBE-PO-DE-05-Pol..._versão final.pdf
Identificação do documento	4cc416c8a25b5dc36a4fbfed60932e9e6aa79ca2
Formato de data da trilha de auditoria	DD / MM / YYYY
Status	● Assinados

Histórico do documento

ASSINADO

12 / 12 / 2023
10:16:30 UTC-3

Assinado por Tânia de Araujo Duprat de Britto Pereira (tania@ccbe.com.br)
IP: 189.37.64.68

VISUALIZADO

12 / 12 / 2023
12:03:30 UTC-3

Visualizado por Walter Luiz Alves de Oliveira Junior (walter.alves@ccbe.com.br)
IP: 189.38.108.93

ASSINADO

12 / 12 / 2023
12:09:09 UTC-3

Assinado por Walter Luiz Alves de Oliveira Junior (walter.alves@ccbe.com.br)
IP: 189.38.108.93

VISUALIZADO

12 / 12 / 2023
13:12:36 UTC-3

Visualizado por Guilherme Bretas Nunes de Lima (guilherme.lima@aliancaenergia.com.br)
IP: 177.199.17.46

Cargo	CCBE-PO-DE-05-Politica de Segurança da informação
Nome de arquivo	CCBE-PO-DE-05-Pol..._versão final.pdf
Identificação do documento	4cc416c8a25b5dc36a4fbfed60932e9e6aa79ca2
Formato de data da trilha de auditoria	DD / MM / YYYY
Status	● Assinados

Histórico do documento

 ASSINADO	**12 / 12 / 2023** 13:13:03 UTC-3	Assinado por Guilherme Bretas Nunes de Lima (guilherme.lima@aliancaenergia.com.br) IP: 177.199.17.46
 ASSINADO	**14 / 12 / 2023** 13:47:39 UTC-3	Assinado por Sandro Magno de Figueiredo e Horta (sandro.horta@aliancaenergia.com.br) IP: 177.190.128.153
 CONCLUÍDO	**14 / 12 / 2023** 13:47:39 UTC-3	O documento foi concluído.