1. OBJETIVO

A Política de Informação da Companhia de Gás do Ceará (Cegás) tem por objetivo regular a classificação das informações segundo critérios de sigilo, definir a estrutura de classificação, orientar sobre as competências e definir responsabilidades no tratamento de informações que agregam valor a sua competitividade e que possam causar impactos no seu desempenho financeiro, participação no mercado, imagem ou no relacionamento com as partes interessadas.

2. ABRANGÊNCIA

As diretrizes de gestão da informação estabelecidas nesta Política deverão ser observadas por todas as áreas da Cegás.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

3.1. Documentos de Referência

- NBR ISO/IEC 17799/2001 - Tecnologia da Informação - Código de prática para a gestão da segurança da informação;
- Lei nº 15.175/2012 - Lei Estadual de acesso à informação;
- Lei nº 13.303/2016 - Disposições aplicáveis às empresas públicas e às sociedades de economia mista;
- Regulamento de Pessoal da Cegás;
- Código de Ética da Cegás.

4. DEFINIÇÕES

Os critérios usados para definir e classificar as informações neste documento tiveram como referência o art. 22, da lei estadual 15.175/2012:

- São consideradas imprescindíveis à segurança da sociedade

ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam, sem prejuízo de dispositivos previstos em lei federal específica:

I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

III - pôr em risco a vida, a segurança ou a saúde da população;

IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

V - prejudicar ou causar risco a planos ou operações estratégicos de órgãos de segurança pública do Estado;

VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico estadual;

VII - pôr em risco a segurança de instituições ou de autoridades estaduais e seus familiares;

VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

Art.23. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.

§1º Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no caput, vigoram a partir da data de sua produção e são os seguintes:

I - ultrassecreta: 25 (vinte e cinco) anos;

II - secreta: 15 (quinze) anos;

III - reservada: 5 (cinco) anos.

§2º As informações que puderem colocar em risco a segurança do Governador e Vice-Governador do Estado e respectivos cônjuges e filhos(as) serão classificadas como reservadas e ficarão sob sigilo até o término do mandato em exercício ou do último mandato, em caso de reeleição.

§3º Alternativamente aos prazos previstos no §1º, poderá ser estabelecida como termo final de restrição de acesso à ocorrência de determinado evento, desde que este ocorra antes do transcurso do prazo máximo de classificação.

§4º Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, a informação tornar-se-á, automaticamente, de acesso público.

§5º Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:

I - a gravidade do risco ou dano à segurança da sociedade e do Estado;

II - o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

Em complemento, seguimos o que diz o inciso 5º, do artigo 85, da Lei 13.303, "os critérios para a definição do que deve ser considerado sigilo estratégico, comercial ou industrial serão estabelecidos em regulamento".

4.1. Informação Ultrassecreta - Classificação atribuída às informações que, se reveladas, podem ocasionar danos graves e irrecuperáveis de nível político ou estratégico, comprometendo os negócios ou a imagem da Companhia, causando reflexos acionários ou ameaças a pessoas e instalações. O prazo máximo de restrição de acesso a este tipo de informação é de 25 anos.

4.2. Informação Secreta

a) as informações que garantem à Companhia a obtenção de vantagens competitivas;
b) as informações que descrevem uma parte significante dos seus negócios;
c) as informações que contêm estratégias operacionais de longo prazo;
d) as informações que têm um impacto potencialmente sério nas políticas e práticas relacionadas a recursos humanos.
e) O prazo máximo de restrição de acesso a este tipo de informação é de 15 anos

4.3. Informação Reservada

a) as informações que garantem à Companhia a manutenção das suas vantagens competitivas;
b) as informações que descrevem uma parte dos seus negócios;
c) as informações que contêm planos operacionais de curto e médio prazo.
d) O prazo máximo de restrição de acesso a este tipo de informação é de 5 anos

4.4. Informação Pública - Classificação atribuída às informações da Companhia que não apresentam potencial de risco e que sua divulgação ao público externo agregue valor à competitividade do negócio e à imagem. São consideradas públicas também as informações que tem divulgação determinadas por lei. As Informações Públicas podem ser disponibilizadas, desde que para o público externo alvo da informação.

4.5. Tratamento das informações - Conjunto de procedimentos relativos ao tratamento de informações e da documentação produzida e/ou recebida pela Companhia, englobando tarefas relativas ao recebimento, elaboração, manuseio, reprodução, divulgação, guarda, transporte, descarte

e criptografia.

4.6. Cifra ou Criptografia - Sistema criptográfico constituído por um algoritmo matemático que, mediante o emprego de uma cadeia de chaves, permite transformar um texto claro em um texto ininteligível e vice-versa.

4.7. Documento secreto - Qualquer documento, sistema de informação ou mídia eletrônica que contenha informação classificada, em relação ao grau de sigilo, como confidencial.

4.8. Documento público - Qualquer documento, sistema de informação ou mídia eletrônica que contenha informação classificada, em relação ao grau de sigilo, como pública.

4.9. Documentos eletrônicos em mídia transportável - Documentos armazenados em mídias tais como disquetes, CDs, DVDs, fitas magnéticas, cartuchos eletrônicos*, flash memories* ou qualquer outro meio eletrônico transportável que exista ou venha a ser criado.

4.10. Lugares públicos - São espaços onde não há privacidade ou controle de acesso, tais como restaurantes, salas de aeroportos, aviões, saguão de hotéis e outros ambientes similares.

5. AUTORIDADE E RESPONSABILIDADE

5.1. Coordenador do Comitê Setorial de Acesso à Informação - Empregado integrante do quadro permanente da Companhia, formalmente designado pela Diretoria Executiva para coordenar as atividades de Acesso à informação.

5.2. Gestor de Segurança da Informação - Gestor da unidade organizacional que origina ou adquire a informação, tornando-se responsável pela sua segurança, ou da unidade organizacional especificamente designada como tal pelo nível gerencial competente.

5.3. Custodiante - Gestor da unidade organizacional responsável pelo armazenamento, processamento, manutenção, recuperação, disponibilização, guarda, transporte e eventual descarte da informação.

5.4. Usuário - Empregado ou contratado autorizado a utilizar informações e recursos de informação da Cegás.

5.5. Contratado - Prestador de serviços que, por contrato, deve permanecer dentro da organização por um período determinado.

A administração da Companhia, nos seus diversos níveis, considera a gestão da informação essencial para a competitividade e o desempenho da Cegás. Para assegurá-la, estabelece e revê periodicamente os princípios de gestão da informação, aloca os recursos organizacionais, humanos e materiais necessários à sua implementação, acompanha os resultados obtidos e determina a aplicação de medidas corretivas.

6. DESCRIÇÃO

6.1. Tratamento a ser observado nas diversas etapas de tramitação de documentos confidenciais

6.1.1. Na etapa de recebimento

Cabe aos responsáveis pelo recebimento de documentos corporativos:

- Verificar, e registrar se for o caso, indícios de violação ou de quaisquer irregularidades na correspondência recebida, dando ciência do fato ao remetente;
- Assinar e datar o respectivo recibo que acompanha o documento, se houver;
- Proceder ao protocolo ou registro do documento em livro ou software adequado a tal finalidade, se necessário;
- Submeter documentos eletrônicos em mídia transportável a software antivírus, rejeitando-os quando verificada a sua existência, dando ciência do fato ao remetente.

6.1.2. Na etapa de elaboração

- Documentos confidenciais devem ser elaborados, necessariamente, nas instalações da Cegás, tomando-se o cuidado de protegê-los de acessos não autorizados;
- Não é permitida a elaboração de documentos confidenciais em lugares públicos.

6.1.3. Na etapa de manuseio

Documentos confidenciais devem ser manuseados, necessariamente, nas instalações da Cegás, tomando-se todos os cuidados, de modo a preservar a sua integridade e o seu sigilo.

6.1.4. Na etapa de reprodução

- É permitida a reprodução de todo ou parte de documento ultrassecreto, secreto ou reservado, se autorizada pelo gestor da informação, devendo a cópia ter o mesmo grau de sigilo do documento original e ser autenticada pelo respectivo gestor;
- O responsável pela reprodução de documentos ultrassecretos, secretos e reservados deve destruir notas, manuscritos, clichês, carbonos, provas ou quaisquer outros elementos que possam dar origem à cópia não autorizada do todo ou de parte;
- A reprodução de documentos ultrassecretos, secretos e reservados deve ser realizada dentro de área apropriada ao seu grau de sigilo;
- Sempre que a preparação para a reprodução de documento ultrassecretos, secretos e reservados for efetuada em tipografias, impressoras ou oficinas gráficas, tal operação deve ser acompanhada por pessoal oficialmente designado, a quem será imputada responsabilidade pela garantia do sigilo;
- A reprodução de documentos ultrassecretos, secretos e reservados em mídia eletrônica transportável somente poderá ser efetuada se autorizada pelo gestor da informação;
- Cada exemplar de documento ultrassecretos, secretos e reservados deve conter uma numeração de controle, de modo a identificar, de forma inequívoca, o seu detentor.

6.1.5. Na etapa de divulgação

- Caso haja necessidade de divulgação para o ambiente externo, os documentos ultrassecretos, secretos e reservados devem ser previamente analisados pelo Comitê Setorial de Acesso à Informação e a aprovação da divulgação deve ser formalizada pelos respectivos gestores e instâncias responsáveis
- É recomendável que a expedição de documentos ultrassecretos, secretos e reservados por meio de correio eletrônico se dê mediante criptografia e com a certificação digital do emissor;
- Não é permitida a transmissão de documentos ultrassecretos, secretos e reservados via fax.

6.1.6. Na etapa de guarda

- Documentos ultrassecretos, secretos e reservados serão guardados em condições especiais de segurança, tais como armários ou gavetas com chaves e, sempre que possível em locais de pouco trânsito de pessoas;
- A guarda de documentos ultrassecretos, secretos e reservados em pasta de servidor deve ser feita seguindo a orientação da TI, que identificará o servidor seguro a ser usado por cada área;
- Não é permitida a guarda de documentos ultrassecretos, secretos e reservados em disco rígido de desktop pessoal;
- Documentos ultrassecretos, secretos e reservados só podem ser guardados em discos rígidos de laptops se criptografados, com a autorização do gestor da informação, e devendo uma cópia ser mantida em servidor seguro;
- Documentos ultrassecretos, secretos e reservados armazenados em mídia eletrônica transportável devem seguir as mesmas recomendações dos itens anteriores.

6.1.7. Na etapa de transporte

- É desaconselhável o transporte de documentos ultrassecretos, secretos e reservados fora das instalações da Cegás, exceto aqueles autorizados pelo gestor da informação;
- É de responsabilidade do usuário no transporte do documento, sobretudo fora das instalações da Cegás, considerar a sensibilidade de seu conteúdo e avaliar os riscos relativos à sua circulação;
- Para o transporte de documentos ultrassecretos, secretos e reservados devem ser observadas as seguintes prescrições:
- No envelope serão inscritos o nome e a função do destinatário, seu endereço completo e, claramente indicado, o grau de sigilo do documento;
- É permitida a expedição de documentos ultrassecretos, secretos e reservados pelo correio, em correspondência expressa registrada, em envelopes próprios que possuam lacre, e acondicionada em um segundo envelope que descaracterize o grau de sigilo.

6.1.8. Na etapa de descarte

- O descarte de documentos e informações de valor legal, classificados como ultrassecretos, secretos e reservados, devem obedecer aos prazos estabelecidos em lei, conforme sua natureza;

- Ocorrendo situação em que a informação ultrassecreta, secreta e reservada não seja mais oportuna, esta deverá ser destruída conforme orientações a seguir:
- Não poderão ser descartados documentos ultrassecretos, secretos e reservados de valor histórico permanente;
- Documentos eletrônicos ultrassecretos, secretos e reservados armazenados em servidores, após a sua exclusão, devem ser eliminados também dos locais de armazenamento temporário, mantidos pelos sistemas operacionais, tipo da lixeira do Windows, quando existirem;
- Documentos confidenciais eletrônicos, impressos ou armazenados em mídias transportáveis, reutilizáveis ou não, devem ser triturados em equipamento apropriado.

6.1.9. Na etapa de criptografia

É vedado o uso de qualquer sistema de cifra ou dispositivo de criptografia que não esteja de acordo com as prescrições corporativas, definidas pela TI e aprovadas pela DIREX.

6.2. Tratamento a ser observado nas diversas etapas de tramitação de documentos ultrassecretos, secretos e reservados **.**

6.2.1. Na etapa de recebimento

Cabe aos responsáveis pelo recebimento de documentos ultrassecretos, secretos e reservados :

- Verificar, e registrar se for o caso, indícios de violação ou de quaisquer irregularidades na correspondência recebida, dando ciência do fato ao remetente;
- Assinar e datar o respectivo recibo que acompanha o documento, se houver;
- Proceder ao protocolo ou registro do documento em livro ou software adequado a tal finalidade, se necessário;
- Documentos eletrônicos em mídia transportável deverão ser submetidos a software antivírus, rejeitando-os quando verificada a sua existência, dando ciência do fato ao remetente.

6.2.2. Na etapa de elaboração

- Documentos ultrassecretos, secretos e reservados devem ser elaborados, necessariamente, nas instalações da Cegás, tomando-se o cuidado de protegê-los de acessos não autorizados;
- Não é permitida a elaboração de documentos em lugares públicos.

6.2.3. Na etapa de manuseio

Documentos **ultrassecretos, secretos e reservados** devem ser manuseados, necessariamente, nas instalações da Cegás, tomando-se todos os cuidados, de modo a preservar a sua integridade e o seu sigilo.

6.2.4. Na etapa de reprodução

É permitida a reprodução de todo ou parte do documento corporativo, devendo a cópia ter o mesmo grau de sigilo do documento original.

6.2.5. Na etapa de divulgação

Caso haja necessidade de divulgação para o ambiente externo, os documentos corporativos devem ser previamente analisados e a aprovação formalizada pelo gestor da informação.

6.2.6. Na etapa de guarda

Documentos corporativos inclusive aqueles gerados em meios magnéticos, devem ser guardados de forma a permitir consulta a posteriori.

6.2.7. Na etapa de transporte

É de responsabilidade do usuário no transporte do documento, sobretudo fora das instalações da Cegás, considerar a sensibilidade de seu conteúdo e avaliar os riscos relativos à sua circulação;

6.2.8. Na etapa de descarte

- O descarte de documentos e informações de valor legal, classificados como ultrassecretos, secretos e reservados , devem obedecer aos prazos estabelecidos em lei, conforme sua natureza;
- Não poderão ser descartados documentos corporativos com valor histórico permanente;
- Documentos eletrônicos corporativos armazenados em mídia transportável, reutilizável deverão ser apagados e após sua exclusão, devem ser eliminados também dos locais de armazenamento temporário, mantidos, pelos sistemas operacionais;
- Documentos corporativos, impressos ou armazenados em mídias transportáveis, reutilizáveis ou não, devem ser triturados em equipamento apropriado.

6.2.9. Na etapa de criptografia

É desaconselhável o uso de criptografia em documentos corporativos.

6.3. Tratamento a ser observado nas diversas etapas de tramitação de documentos públicos.

6.3.1. Na etapa de recebimento

Cabe aos responsáveis pelo recebimento de documentos público:

- Verificar, e registrar se for o caso, indícios de violação ou de quaisquer irregularidades na correspondência recebida, dando ciência do fato ao remetente;
- Assinar e datar o respectivo recibo que acompanha o documento, se houver;
- Proceder ao protocolo ou registro do documento em livro ou software adequado a tal finalidade, se necessário;
- Documentos eletrônicos em mídia transportável deverão ser submetidos a software antivírus, rejeitando-os quando verificada a sua existência, dando ciência do fato ao remetente.

6.3.2. Na etapa de elaboração

- Documentos públicos devem ser elaborados, necessariamente, nas instalações da Cegás.
- Não é permitida a elaboração de documentos em lugares públicos.

6.3.3. Na etapa de manuseio

Documentos públicos podem ser manuseados livremente.

6.3.4. Na etapa de reprodução

É permitida a reprodução de todo ou parte de documento público.

6.3.5. Na etapa de divulgação

Documentos públicos podem ser divulgados para o ambiente externo, desde que respeitadas as restrições para sua liberação, estabelecidas pela Cegás.

6.3.6. Na etapa de guarda

Documentos públicos inclusive aqueles gerados em meios magnéticos, devem ser guardados de forma a permitir consulta a posteriori.

6.3.7. Na etapa de transporte

Os documentos públicos podem ser transportados livremente.

6.3.8. Na etapa de descarte

- O descarte de documentos e informações de valor legal, classificados como públicos, devem obedecer aos prazos estabelecidos em lei, conforme sua natureza;
- Não poderão ser descartados documentos corporativos com valor histórico permanente.

6.3.9. Na etapa de criptografia

É desaconselhável o uso de criptografia em documentos públicos.

6.4. Penalidades

- O tratamento indevido de documentos é considerado como falta grave e implicará na aplicação de sanções disciplinares, conforme estabelecido no Regulamento de Pessoal e no Código de Ética da Companhia;
- As penalidades decorrentes da inobservância do presente procedimento podem variar entre advertência escrita, suspensão ou rescisão do contrato de trabalho, devendo ser considerados para sua aplicação os seguintes elementos: a natureza e a gravidade da falta, os danos que dela provierem para a Área isoladamente ou para a Companhia como um todo e, principalmente, as circunstâncias em que a falta se verificou;
- As penalidades são extensivas a contratados, a terceiros, bem como, a outras pessoas que, por força de parcerias e ou contratos, prestem serviços à Cegás.

6.5. Competência para classificação

- A competência para a classificação das informações, segundo o seu grau de sigilo, é do seu respectivo gestor. Para identificar o valor da informação de natureza sigilosa de forma a classificá-la adequadamente, o gestor buscará estabelecer o consenso pelos usuários da informação;
- Observando a tabela a seguir, se a classificação proposta estiver na competência do coordenador setorial de acesso à informação, ele a classificará. Caso contrário, o gestor submeterá a classificação para aprovação ao nível hierárquico superior adequado correspondente.

- **A Cegás deverá, uma vez identificada as informações, encaminhar a proposta de classificação ao Comitê Gestor de Acesso à Informação e ao Conselho Estadual de Acesso à Informação, para deliberação sobre o assunto.**

6.5.1. Competência para classificação de informações

- **Ultrassecretos, secretos e reservados** – Conselho de Administração (CONAD) e Diretoria Executiva (DIREX);
- **Pública** – DIREX e Gestores, tanto para informações de impacto abrangente, como para aquelas de impacto local consideradas, neste último caso, as diretrizes de comunicação institucional e de relacionamento com o mercado da Companhia.

Diretrizes orientadoras sobre a identificação do valor da informação, em nível corporativo ou da unidade organizacional correspondente, poderão ser elaboradas pela DIREX à medida que tal necessidade for identificada.

6.6 Premissas Básicas

Além dos princípios constantes da Política de Segurança da Informação da Cegás, são aplicáveis as seguintes premissas:

- Ao atribuir um grau de sigilo, o gestor da informação deve buscar um equilíbrio entre a necessidade de sigilo e os custos das medidas de proteção. Um grau de sigilo exagerado compromete a velocidade de transmissão da informação e contribui para a saturação dos sistemas de processamento e o desperdício nos recursos. Um grau de sigilo inferior ao adequado gera vulnerabilidades para o negócio;
- A classificação de uma informação deve ser preservada pelo prazo imposto por lei ou até atingir a obsolescência, após o que deve ser submetida a procedimentos de arquivo ou descarte;
- Uma informação poderá ter o seu grau de sigilo modificado por autoridade de nível hierárquico superior ao do seu gestor. Nesse caso, o gestor da informação deve ser alertado para a adoção das medidas de proteção decorrentes da mudança;
- Caso algum Gestor julgue que a classificação de uma informação seja inadequada, a nova classificação deve ser proposta, aumentando-se ou diminuindo-se a respectiva classificação, remetendo-a, se necessário, para a apreciação da autoridade classificadora original;
- A classificação da informação deve estar identificada e de fácil visualização;

- As informações da Cegás devem ser consideradas como corporativas até que sejam classificadas por seus respectivos gestores, salvo quando já tiverem sido pré-classificadas;
- O acesso a informações **ultrassecretos, secretos e reservados** só será admitido aos usuários que, no exercício de função ou atividade, tenham a necessidade de conhecê-las;
- Considerando o grau de sigilo, os gestores especificam formalmente os usuários das informações sob sua responsabilidade;
- Compete aos gestores, em suas respectivas áreas de atuação, definir o conjunto de informações classificáveis como **ultrassecretos, secretos e reservados** ou Pública;
- Algumas informações de interesse específico da pessoa a que se destina e, para que não sejam abertas ou manuseadas por terceiros, deverão levar a indicação “PESSOAL”, além da classificação quanto ao grau de sigilo.

6.7. Responsabilidade e desenvolvimento da Política

6.7.1. Conselho de Administração

Na condição de integrante da Administração da Companhia, é responsável pela aprovação da Política de Segurança da Informação da Companhia, bem como das suas atualizações.

6.7.2. Diretoria Executiva

Na condição de integrante da Administração da Companhia, é responsável por encaminhar ao Conselho de Administração as propostas de atualização da presente Política de Segurança da Informação da Companhia, bem como por implantar e garantir o cumprimento da mesma nos diversos níveis da Organização.

6.7.2.1. Além disso, a Diretoria Executiva possui as seguintes responsabilidades inerentes à Segurança da Informação:

- Coordenar, orientar e avaliar as atividades relativas à segurança da informação na Cegás, promovendo ações de interesse corporativo;
- Estabelecer e manter atualizadas as normas, as diretrizes, os procedimentos e outros documentos relacionados à aplicação da presente Política, sempre que possível em articulação com as partes interessadas;
- Promover programas educacionais e de comunicação relacionados à segurança da informação na Cegás;
- Promover auditorias para verificar o cumprimento da política, das normas, das diretrizes, dos

procedimentos e outros documentos afins de segurança da informação;

- Estabelecer os Indicadores de Segurança da Informação a serem utilizados e acompanhar seus resultados junto às áreas da organização;
- Promover ações de melhoria da Segurança da Informação na Cegás;
- Definir as medidas apropriadas para controlar a circulação de pessoas e equipamentos nas instalações da Cegás;
- Acompanhar as ações adotadas pelas áreas da Companhia para investigação e apuração de incidentes relativos a Segurança da Informação; e
- Acompanhar estudos de implantação de novas tecnologias e seus possíveis impactos no que tange a Segurança da Informação.

6.7.3. Gestores

As responsabilidades dos ocupantes de todos os cargos de gestão no que tange a Segurança da Informação são as seguintes:

- Assessorar a Diretoria Executiva nas questões relativas à segurança da informação;
- Garantir o cumprimento da Política de Segurança da Informação da Cegás, bem como das normas, diretrizes e procedimentos a ela relacionados, por parte dos usuários sob sua responsabilidade;
- Divulgar a Política de Segurança da Informação na Cegás e implantar as orientações da Diretoria Executiva em todas as unidades da Companhia;
- Coordenar programas de identificação, educação e conscientização de usuários de sua área de atuação;
- Coordenar a identificação de vulnerabilidades da sua área e a implantação de um plano de segurança da informação para solucioná-las, relatando à Diretoria Executiva as ocorrências e as práticas relevantes;
- Avaliar a eficácia da segurança da informação na sua área, reportando à Diretoria Executiva os resultados dos indicadores;
- Garantir a inclusão de cláusulas contratuais que assegurem a observância desta Política de Segurança da Informação;
- Aplicar as ações corretivas e disciplinares nos casos de quebra de segurança de informações por usuários sob sua responsabilidade;
- Informar as movimentações de usuários sob sua responsabilidade aos gestores e

custodiantes; e

- Reportar à Diretoria Executiva as situações que possam comprometer a segurança das informações da Companhia.

6.7.4. Gestores de Segurança da Informação

São denominados Gestores de Segurança da Informação os gerentes de cada área onde existe produção de informações cujas responsabilidades incluem:

- Identificar e classificar as informações sob sua responsabilidade;
- Definir as necessidades de segurança para as informações sob sua responsabilidade;
- Assegurar a adoção de medidas adequadas de segurança das informações sob sua responsabilidade;
- Conceder as autorizações de acesso às informações sob sua responsabilidade, promovendo revisões periódicas das autorizações concedidas;
- Garantir que os custodiantes tenham pleno conhecimento desta Política e das necessidades de segurança para as informações sob sua responsabilidade;
- Participar da elaboração do plano de prevenção e recuperação das informações sob sua responsabilidade, para situações de contingência;
- Solicitar a aplicação de ações corretivas e disciplinares ao gestor do usuário responsável pela quebra de segurança de informações sob sua responsabilidade; e
- Informar a Diretoria Executiva sobre situações que comprometam a segurança das informações sob sua responsabilidade.

6.7.5. Usuários

As responsabilidades dos Usuários relativas à Segurança da Informação estão descritas a seguir:

- Cumprir a Política de Segurança da Informação da Cegás;
- Reportar ao gestor imediato sobre situações que possam comprometer a segurança das informações da Cegás.

6.7.6. Gerência de desenvolvimento humano e organizacional

As responsabilidades da Gerência de Desenvolvimento Humano e Organizacional relativas à Segurança da Informação estão descritas a seguir:

- Manter disponíveis informações atualizadas sobre a lotação dos empregados;

- Assessorar os gestores na aplicação das ações disciplinares previstas para os casos de incidentes relativos a segurança de informações na Cegás.

6.7.7. Assessoria Jurídica

As responsabilidades da **Assessoria Jurídica** relativas à Segurança da Informação estão descritas a seguir:

- Orientar as áreas integrantes da estrutura organizacional da Cegás para que todos os contratos incluam cláusulas que assegurem a observância do prescrito no presente documento;
- Assessorar as áreas integrantes da estrutura organizacional da Companhia na aplicação de sanções legais em caso de incidentes de segurança de informações que envolvam a Cegás.

6.7.8. Auditoria (Interna ou Externa)

A Auditoria, interna ou externa, relativa a Segurança da Informação será determinada periodicamente pela Diretoria Executiva, e terá por objetivo informar sobre a existência situações que possam, de alguma forma, comprometer a segurança das informações da Cegás.

6.7.9. Informações Relevantes

- Caberá ao Gerente de Planejamento zelar para que as Informações Relevantes ocorridas ou relacionadas aos negócios da Cegás sejam divulgadas na forma prevista nesta Política, de forma clara e precisa, em linguagem acessível ao público;
- A divulgação das Informações Relevantes será articulada pela Assessoria de Comunicação e Marketing e ocorrerá por meio da publicação de anúncios nos jornais de grande circulação, Diário Oficial do Estado e site da Companhia utilizados habitualmente pela Cegás, podendo o anúncio conter uma descrição resumida da informação relevante e indicar os endereços na rede mundial de computadores (Internet) onde a informação detalhada deverá estar disponível;
- As Pessoas Vinculadas que tenham conhecimento de qualquer fato que possa configurar Informação Relevante deverá comunicar, imediatamente e por escrito, ao Gerente de Planejamento para que este, por sua vez, tome as medidas necessárias para divulgação da referida informação, nos termos desta Política;
- As Pessoas Vinculadas que tenham conhecimento de Informação Relevante e constatem a omissão do Gerente de Planejamento no cumprimento de seu dever encaminha imediatamente comunicação escrita aos Administradores da Cegás para que estes tomem as medidas cabíveis

para divulgação da informação. A responsabilidade dos Administradores e das Pessoas Vinculadas que tiverem acesso a Informações Relevantes não divulgadas apenas cessará quando da sua efetiva divulgação;

6.8. Disposições Gerais

A presente Política de Segurança da Informação da Cegás será complementada por diretrizes, normas, procedimentos e outros documentos afins, considerados partes integrantes desta Política, e cuja competência de aprovação é da Diretoria Executiva.

6.9. Aplicação

A responsabilidade por Segurança da Informação deve ser assumida pela organização como um todo, o que inclui os seus Administradores, os seus Acionistas, os seus gestores e colaboradores, além de seus fornecedores e parceiros.

7. REGISTROS

Identificação	Armazenamento	Grau de Sigilo	Proteção	Recuperação	Retenção	Disposição
Política de Gestão da Informação	Meio Eletrônico/ físico	Corporativo	Back up/pasta	Nome	Indeterminado	Não aplicável (N/A)

Versão	**Data**	**Histórico**	**Aprovação**
00		Emissão de Documento	

8. ANEXOS

Não aplicável.