

	SISTEMA DE NORMALIZAÇÃO CORPORATIVA	
	SUBSISTEMA POLÍTICAS ORGANIZACIONAIS	
	Diretoria: Administração e Finanças	Vigência: 25/10/2018
	Área de origem: Gerência de Tecnologia e Sistemas de Informação	Revisão: 00
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		Página: 1 de 4

1. OBJETIVO

Estabelecer os princípios, normas e responsabilidades relativos à Segurança da Informação na Companhia.

2. ABRANGÊNCIA

Toda a Companhia.

3. DEFINIÇÕES

Administrador de acesso – Responsável pelo controle de acesso às informações por outras pessoas ou entidades.

Ameaça – São agentes ou condições causadoras de incidentes contra ativos, de informação ou de outra natureza. Exploram as vulnerabilidades, ocasionando perda de suas características.

Análise de Riscos – É a identificação das medidas de segurança cabíveis, visando identificar ativos, suas vulnerabilidades, ameaças e impactos de alterações em suas características.

Controle de acesso – Administração do direito de acesso e de divulgação de informações, independente do meio em que estejam, envolvendo: permissão, verificação e exclusão de direitos de visualização e/ou alteração.

Colaborador – é todo profissional que esteja exercendo funções laborais em benefício ou proveito da COMPAGAS, tais como: empregado, diretor, empregado cedido por acionista, e profissionais pertencentes às empresas contratadas.

Direito de Acesso – Privilégio associado a uma pessoa, cargo, função, ou processo para acesso a um ativo, que não implica no direito de divulgação.

Dever de Diligência – Toda atenção ou cuidado que deve ser aplicado pela pessoa que executa um ato ou procede a um negócio, para que tudo se cumpra com a necessária regularidade.

Direito de Divulgação – Privilégio associado a uma pessoa, cargo, função ou processo para divulgação de informação, independente do meio ou forma.

Informação - Ativo da Companhia, expresso de forma impressa, escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas, que necessita, por sua importância, ser adequadamente protegido, manuseado e gerenciado.

Características da Informação

- **Confidencialidade** – garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.
- **Conformidade** – a informação está em conformidade com leis, regulamentações e acordos contratuais aos quais o processo de negócio está submetido.

- **Disponibilidade** – garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Efetividade** – a informação é relevante e pertinente para o processo de negócio, e é disponibilizada no momento adequado de forma utilizável e de uma maneira correta e consistente.
- **Eficiência** – a informação é disponibilizada através da utilização otimizada (mais produtiva e econômica) de recursos.
- **Integridade** – salvaguarda da exatidão e completeza da informação e dos métodos de processamento.
- **Confiabilidade** – a informação retrata a realidade operacional e financeira da corporação.

Rastreabilidade - Característica da informação que possibilita acompanhar ou identificar algo durante um processo: saber "o quê", "quem", "quando", de "onde" e "para onde"

Segurança da informação – Conjunto de diretrizes, instrumentos e ações que garantem a confidencialidade, a disponibilidade e a integridade das informações.

Termo de Responsabilidade e Sigilo – Instrumento por meio do qual é confirmado o conhecimento das normas relativas à segurança da informação e é atribuída responsabilidade individual pela preservação da segurança da informação da Companhia ou sob sua guarda.

Vulnerabilidade – São fragilidades associadas aos ativos, de informação ou de outra natureza, que os tornam suscetíveis a ameaças.

4. DESCRIÇÃO

4.1 PRINCÍPIOS

Os seguintes princípios de proteção da informação devem ser aplicados em todas as normas, ações e processos da Companhia:

I - princípio dos "Direitos Mínimos": às pessoas caberá acessar apenas os ativos que garantam o desenvolvimento de suas atividades;

II - princípio da "Exposição Mínima" – manter protegida a informação, sendo exposta apenas quando necessária.

4.2 DIRETRIZES

4.2.1 - Toda informação produzida ou incorporada pela COMPAGAS é de sua propriedade, sendo parte de seu patrimônio como ativo intangível.

4.2.2 - A informação será protegida pelos níveis de autoridade formal, estabelecidos pela COMPAGAS, sendo exposta de acordo com a necessidade.

4.2.3 - Todas as características de segurança da informação devem ser preservadas na COMPAGAS.

4.2.4 - Os processos e sistemas de informação devem atender às exigências de rastreabilidade para alterações e acessos às informações.

4.2.5 - Todo acesso e uso da informação deve ser realizado com dever de diligência, respondendo pela ação ou omissão, de acordo com as Normas Internas, Código de Conduta e Integridade, Estatuto Social e Legislação.

4.3. RESPONSABILIDADES

4.3.1 DA COMPAGAS

É responsabilidade da Companhia de acordo com suas atribuições e competências:

- I - promover a cultura de Segurança da Informação;
- II - capacitar o quadro funcional para a plena utilização das ferramentas de segurança de acordo com suas atividades;
- III - divulgar informações relativas à proteção das informações, às ferramentas e à solução de problemas de segurança;
- IV - garantir proteção adequada às informações da Companhia ou sob sua guarda;
- V - identificar de forma inequívoca todo aquele que acessa a informação;
- VI - proteger os equipamentos que tratam as informações da Companhia e as instalações que abrigam estes, de danos acidentais, naturais ou dolosos e acesso não autorizado;
- VII - segregar responsabilidades, implantando mecanismos de controle sobre as atividades e direitos de acesso e de divulgação;
- VIII - assegurar e monitorar o uso correto das informações disponíveis na Companhia coibindo o acesso e divulgação não autorizados;
- IX - fazer constar em todas as formas de contratos requisitos de segurança para acesso e divulgação da informação disponibilizada pela Companhia;
- X - prover mecanismos para recuperação das informações, conforme análise de riscos;
- XI - prover mecanismos para identificação e rastreamento das atividades de acesso e alteração de informações, conforme análise de riscos;
- XII - inventariar e cadastrar as informações e os usuários detentores da informação.

4.3.2 DOS COLABORADORES

É responsabilidade dos colaboradores:

- I - seguir os procedimentos de segurança da Informação definidos pela Companhia;
- II - acessar e utilizar as informações somente quando autorizado e apenas para atividades aprovadas pela Companhia;
- III - salvaguardar as características da informação sob sua guarda, em qualquer formato e meio de armazenamento, tanto no ambiente de trabalho como fora deste, envolvendo, mas não se limitando a:
 - a) impedir o acesso às informações nos momentos em que não as estiver utilizando;
 - b) permitir o acesso às informações somente a pessoas autorizadas;
 - c) não divulgar informações sem autorização da Companhia;
- IV - não copiar nem remover informação do meio de armazenamento definido pela Companhia, sem sua autorização;
- V - comunicar a Companhia qualquer incidente de segurança da informação.

5. REFERÊNCIAS

Norma ABNT NBR ISO/IEC 27001

Política de Segurança da Informação (Versão 07 de 22.12.2017) - Copel (Holding) e suas subsidiárias integrais

6. SUBSTITUIÇÃO DE VERSÃO

Não se aplica.

7. APROVAÇÃO E VIGÊNCIA

Esta Política foi aprovada na 151ª reunião do Conselho de Administração, de 25/10/2018, com vigência a partir desta data.

8. ANEXOS

Não se aplica.