

Elaborado por:	Sandra Barreiros
Aprovado por:	Rita d'Araújo
Data última atualização:	06 de abril de 2020
Alterações:	Versão inicial



POLÍTICA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

INDICE

1. POLÍTICA DE GESTÃO DE SEGURANÇA DE INFORMAÇÃO.....	1
2. ORGANIZAÇÃO E RESPONSABILIDADE	2
3. GESTÃO DOS NOSSOS RECURSOS HUMANOS.....	2
4. GESTÃO DOS NOSSOS ATIVOS E REPOSITÓRIOS DE INFORMAÇÃO	3
5. CATÁLOGO DE NORMAS, POLÍTICAS E PROCEDIMENTOS APLICÁVEIS E EM VIGOR NA ORGANIZAÇÃO (ITG)	3
6. DOCUMENTOS DE SUPORTE.....	3
7. DEFINIÇÕES	3
8. SIGLAS, ACRÓNIMOS E ABREVIATURAS.....	4

1. POLÍTICA DE GESTÃO DE SEGURANÇA DE INFORMAÇÃO

Estamos cientes da elevada importância da informação para a nosso grupo, para os nossos colaboradores, para os nossos parceiros e para os nossos clientes. Incorporamos, tratamos e protegemos a informação própria e a que nos é confiada, impedindo a sua divulgação, adulteração ou alteração não controlada.

Esta **política de segurança da informação** deve ser analisada de forma crítica, em intervalos regulares, planeados e sempre que ocorram mudanças significativas, assegurando a sua contínua pertinência, adequação e eficácia.

O **ITG, Instituto Tecnológico do Gás**, doravante designado de **ITG**, consciente e preocupado com a sua credibilidade e reputação, aposta e investe no reforço da fiabilidade e da resiliência daquilo que representa o seu negócio, a segurança da sua informação e a segurança da informação dos seus clientes e parceiros.

O âmbito desta **Política** e normativos consequentes endereça os seguintes tópicos (não exaustivo):

- Gestão da segurança de informação;

- Gestão de ativos;
- Segurança em recursos humanos;
- Segurança física e do ambiente;
- Gestão de operações e comunicações;
- Controlo de acessos;
- Aquisição, desenvolvimento e manutenção de sistemas da informação;
- Gestão de incidentes de segurança da informação;
- Gestão de continuidade de negócio;
- Conformidade.

2. ORGANIZAÇÃO E RESPONSABILIDADE

A **Política de Segurança** da Informação é da responsabilidade do *CISO – Chief Information Security Officer* ou, na sua ausência, do *Conselho de Administração*, cabendo-lhe o controlo e a avaliação da implementação do *Sistema de Gestão de Segurança da Informação (SGSI)*, a comunicação à gestão de topo do seu desempenho, o contacto com as diferentes áreas e empresas do grupo e respetivos órgãos hierárquicos para adequação dos mesmos e a garantia da conformidade do sistema com os requisitos dos normativos aplicáveis.

As medidas de segurança devem ser técnica e economicamente viáveis e não devem limitar de forma inadequada a produtividade e eficiência do **ITG**.

A implementação, validação e a melhoria contínua destas medidas é responsabilidade de todos, nomeadamente:

- Na proteção dos recursos e observação das boas-práticas em vigor na organização;
- Ao observar o cumprimento das regras de acesso físico e lógico, reportando qualquer comportamento anómalo de forma pronta e construtiva;

- Ao cumprir e fazer cumprir os princípios da segregação e acessos e funções.

Na medida do possível promovemos e mantemos pontos de coordenação para o intercâmbio e troca de informação entre o **ITG** e:

- Autoridades Judiciais, legais ou regulatórias;
- Grupos de interesse.

Observamos, promovemos e cumprimos de forma consistente os princípios de:

- Segurança e Privacidade por Defeito;
- Segurança e Privacidade na Conceção.

Promovemos, otimizamos e asseguramos a nossa mobilidade, procurando implementar e fazer cumprir iguais princípios de:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Autenticidade;
- Prova.

Promovendo uma adequada gestão de incidentes e uma cultura de resiliência e de continuidade de negócio.

3. GESTÃO DOS NOSSOS RECURSOS HUMANOS

Avaliamos e verificamos as referências dos nossos candidatos, cumprindo e fazendo cumprir todas as nossas obrigações de privacidade, proteção de informação pessoal e toda a legislação laboral vigente.

Mantemos atualizados todos os descritivos de funções e responsabilidades vigentes na **ITG**, promovendo uma consciencialização e formação contínua na forma como cada colaborador deve desempenhar as suas tarefas e funções de forma segura e eficaz.

Promovemos uma validação periódica dos nossos acessos, assegurando que cada

colaborador detém acesso à informação relevante para o correto e eficaz desempenho das suas funções, promovendo simultaneamente o princípio do **Privilegio Mínimo**, validando e promovendo igualmente os nossos cuidados na segregação de funções e responsabilidades.

4. GESTÃO DOS NOSSOS ATIVOS E REPOSITÓRIOS DE INFORMAÇÃO

Registamos e mantemos atualizados os inventários de documentos e registos que gerimos. Formalizamos, potenciamos e promovemos a gestão cuidada dos nossos ativos. A cada grupo de ativos e repositórios são autorizados, atribuídos, validados, restringidos e cancelados acessos com base em orientações de uma área responsável, devendo esta adequar com o Conselho de Administração a forma e os meios que operacionalizam e implementam os controlos identificados.

O responsável deverá desenvolver os melhores esforços no sentido de:

- Providenciar os meios necessários para que a Política de Segurança de Informação seja conhecida e entendida por todos os Colaboradores;
- Detetar incumprimentos das Normas de Segurança, para que sejam aplicadas medidas corretivas;
- Verificar continuamente a adequação das Normas estabelecidas às necessidades de cada momento, solicitando os procedimentos necessários para garantir a sua atualização e manutenção.

Os Colaboradores são responsáveis por proteger a informação a que têm acesso, salvaguardando que:

- Não a utilizarão em funções não aprovadas;
- Não a divulgarão a pessoas que não estejam autorizadas a aceder à mesma.

Como parte do processo de reconhecimento destas diretivas, as mesmas devem ser comunicadas aos intervenientes, devendo ser cumpridas com rigor todas as regras de segurança aprovadas.

5. CATÁLOGO DE NORMAS, POLÍTICAS E PROCEDIMENTOS APLICÁVEIS E EM VIGOR NA ORGANIZAÇÃO (ITG)

Toda a informação referente a normas, regulamentação, metodologias e Melhores Práticas aplicadas e/ou a aplicar, assim como, o conjunto de Políticas e Procedimentos em vigor e a considerar na Organização (ITG), encontram-se referenciados no documento **ANEXO A: ORIENTAÇÕES - NORMAS, REGULAMENTAÇÃO, BEST PRACTICES, POLÍTICAS E PROCEDIMENTOS APLICÁVEIS**, o qual servirá como **Índice**.

Para o efeito, este documento deverá ser mantido atualizado e, sempre que se justifique, ser revisto.

6. DOCUMENTOS DE SUPORTE

Anexo A: Orientações | Normas, Regulamentação, *Best Practices*, Políticas E Procedimentos Aplicáveis

7. DEFINIÇÕES

Ativo

Qualquer recurso / objeto (tangível ou intangível) indispensável ao funcionamento da Organização

Informação

É um recurso que, como outros importantes recursos de negócios, tem valor para uma organização e por conseguinte precisa ser protegido adequadamente [BS 7799-1: 1999, *British Standards Institute*]

Segurança de Informação	A SI é caracterizada pela preservação da confidencialidade, integridade e disponibilidade. [BS 7799 -1: 1999, British Standards Institute]
Confidencialidade	Propriedade que limita o acesso à informação somente às entidades legítimas (autorizadas pelo proprietário da informação)
Integridade	Propriedade que garante que a informação manipulada mantém todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente).
Disponibilidade	Propriedade que garante que a informação está sempre disponível para o uso legítimo, i.e., pelos utilizadores autorizados pelo proprietário da informação.
Autenticidade	Propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
Least Priviledge	Princípio limitativo de segurança que consiste em facultar unicamente acessos necessários à execução das tarefas estipuladas

8. SIGLAS, ACRÓNIMOS E ABREVIATURAS

CISO	Responsável de Segurança de Informação – Chief Information Security Officer
ITG	Instituto Tecnológico do Gás.
SGSI	Sistema de Gestão de Segurança de Informação
UE	União Europeia

