Gas Solutions

# POLÍTICA DE

# SEGURANÇA DA INFORMAÇÃO

Página em Branco

INDICE

## 1. OBJETIVO

O objetivo deste documento é definir regras claras para o uso do sistema de informação e outros ativos de informação da PRF-Gás, Tecnologia e Construção, S.A.

Os destinatários deste documento são todos os colaboradores da PRF.

## 2. APLICAÇÃO

Segurança na informação da empresa

## 3. DESCRIÇÃO

**Sistema de Informação** – inclui todos os servidores e equipamentos cliente, infraestrutura de rede, software de sistema e aplicações, dados e outros subsistemas de computador e componentes que são propriedade ou usados pela organização. O sistema de informação também inclui o uso de todos os serviços internos ou externos, como acesso à Internet, correio eletrónico, etc.

**Ativos de informação** – no contexto desta política, o termo "ativos de informação" é aplicado a sistemas de informação e outras informações/equipamentos, incluindo documentos em papel, telefones móveis, computadores portáteis, meios de armazenamento de dados, etc.

### 3.1 Utilização aceitável

Os ativos de informação só podem ser utilizados para tarefas relacionadas com necessidades da organização.

### 3.2 Responsabilidade pelos ativos

Cada ativo de informação tem um responsável designado no inventário de ativos. O responsável pelo ativo tem que garantir a confidencialidade, integridade e disponibilidade da informação no recurso em questão.

### 3.3 Atividades proibidas

É proibido usar ativos de informação de modo a enfraquecer o desempenho do sistema de informação ou em ações que podem representar uma ameaça à segurança.

Também é proibido:

- transferir ficheiros de imagem ou vídeo que não tenham um propósito comercial, enviar cartas em cadeia por correio eletrónico, jogar jogos, etc.;

- instalar software no computador local sem permissão explícita do Departamento Informático;
- usar aplicações Java e Active X sem autorização do Departamento Informático;
- usar ferramentas de criptografia no computador local;
- transferir programas de fontes externas;

### 3.4 Deslocação dos ativos para fora das instalações

Não podem ser retirados das instalações, sem a autorização prévia do Responsável da Área, equipamentos, informações ou software, independentemente de seu formato ou meio de armazenamento.

Enquanto esses ativos estiverem fora da organização, estes devem ser controlados pela pessoa a quem foram confiados.

### 3.5 Devolução de ativos após a rescisão do contrato de trabalho

Após a rescisão de um contrato de trabalho todos os ativos de informação (equipamentos e software) devem ser entregues ao Departamento Informático (as informações em formato eletrônico ou em papel devem ser entregues ao Responsável da Área).

### 3.6 Procedimento para as cópias de segurança

Os utilizadores devem conhecer o método e o procedimento para as cópias de segurança de todas as informações confidenciais armazenadas em seu computador. O procedimento para as cópias de segurança deve ser executado pelo menos uma vez por dia.

### 3.7 Proteção Antivírus

O software antivírus deve ser instalado em cada computador com atualizações automáticas ativadas.

As ferramentas de segurança, como o antivírus, não devem ser desativadas.

Este processo encontra-se descrito no PG6 – Controlo de documentos

### 3.8 Procedimento em caso de vírus

Quando um utilizador deteta que o seu equipamento esta infetado deve:

- Desligar qualquer tipo de rede (LAN, Wifi, 3G, 4G) de acesso internet e local.
- Comunicar com o departamento de informática com urgência para que o vírus não danifique todo o equipamento.

### 3.9 Autorização para uso do sistema de informação

Os utilizadores do sistema de informação só podem aceder aos ativos do sistema de informação para os quais foram explicitamente autorizados pelo proprietário do ativo.

Os utilizadores podem usar o sistema de informação apenas para os fins para os quais foram autorizados, ou seja, para os quais receberam explicitamente direitos de acesso.

Os utilizadores não devem participar de atividades que possam ser usadas para contornar controlos de segurança do sistema de informação.

### 3.10 Responsabilidades da conta de utilizador

O utilizador não deve, direta ou indiretamente, permitir que outra pessoa use os seus direitos de acesso, ou seja, nome de utilizador e senha, e não deve usar o nome de utilizador e senha de outra pessoa.

O proprietário da conta de utilizador é o responsável pelo seu uso e por todas as transações realizadas por meio dessa conta de utilizador.

### 3.11 Senhas de acesso

Todas as senhas de acesso devem ser fortes. As regras relativas às senhas encontram-se na IT 22.3 Senhas e Bloqueio de equipamentos.

### 3.12 Proteção de ecrã

Esta referenciado no documento IT 22.14 Secretaria Limpa e ecrã limpo

### 3.13 Utilização de Internet

O acesso à Internet pode ser feito através da rede local da organização, com infraestrutura apropriada e proteção de "firewall".

Por uma questão de segurança, a utilização dos ativos da organização poderá ser monitorizada.

O Responsável pela Segurança TI pode bloquear o acesso a algumas páginas da Internet para utilizadores individuais, grupos de utilizadores ou todos os colaboradores da organização.

Se o acesso a algumas páginas da web for bloqueado, o utilizador pode enviar por escrito um pedido de autorização de acesso a tais páginas para o Responsável pela Segurança TI. O utilizador não deve tentar contornar essa restrição de forma autónoma.

O utilizador deve considerar as informações recebidas por meio de sites não verificados como não confiáveis. Tais informações podem ser usadas para fins comerciais somente após a sua autenticidade e correção terem sido verificadas.

Caso seja necessária a utilização de sites que não sejam automaticamente verificados como confiáveis, poderá ser dada indicação explícita pelo Responsável da Área.

O utilizador é responsável por todas as possíveis consequências decorrentes do uso não autorizado ou inadequado de serviços ou conteúdo da Internet.

### 3.14 Correio eletrónico e outros métodos de troca de mensagens

Os métodos de troca de mensagens além do correio eletrônico também incluem a transferência de ficheiros da Internet, transferência de dados via Web Transfer, telefones, envio de mensagens de texto SMS, unidades portáteis, fóruns e redes sociais.

De acordo com IT 22.6 Procedimentos Operacionais TI Comunicação Ed.0.doc, bem como com IT 22.4 Classificação da Informação - Ed.0.doc, o Responsável pela Segurança TI determina o canal de comunicação que pode ser usado para cada tipo de dados bem como possíveis restrições.

Os utilizadores só podem enviar mensagens contendo informações verdadeiras. É proibido enviar materiais com conteúdo perturbador, desagradável, sexualmente explícito, rude, calunioso ou qualquer outro conteúdo inaceitável ou ilegal. Os utilizadores não devem enviar mensagens de spam para pessoas com quem nenhuma relação comercial foi estabelecida ou para pessoas que não solicitaram tais informações.

Se um utilizador receber um correio eletrónico de spam, deve informar o Responsável pela Segurança TI.

Se enviar uma mensagem classificada como confidencial, o utilizador deve protegê-la.

O utilizador deve guardar as mensagens contendo dados importantes para o negócio da organização usando o método especificado pelo Responsável da Área.

Cada mensagem de correio eletrónico deve conter um aviso legal, exceto as mensagens enviadas por meio de sistemas de comunicação. Se um utilizador publicar uma mensagem num sistema de troca de mensagens (redes sociais, fóruns, etc.), ele deve declarar inequivocamente que não representa o ponto de vista da organização.

### 3.15 Eliminação e reutilização segura de equipamentos da organização.

O método de eliminação dos dados é feito por copia do equipamento para uma pasta de backups no onexafe, A reutilização dos equipamentos em caso de avaria é realizada o desmantelamento de componentes que ainda podem ser utilizados para outro desde que estejam operacionais.

O mecanismo para eliminação dos dados antes da reutilização passa por:

- Guardar os dados do equipamento com retenção de 60 dias.
- Formatar completamente os disco HDD\ SSD para sua reutilização.
- Repor o sistema operativo na forma inicial de utilização.

### 3.16 Procedimentos para a manutenção de equipamentos

Ao realizar a manutenção nos equipamentos o utilizador deve garantir que os ficheiros ou pastas da organização se encontram no servidor.

O procedimento de manutenção de equipamento é seguido com a lista de manutenção de equipamentos onde é verificado o dispositivo de forma assegurar o bom funcionamento e a verificação de falhas de segurança.

A manutenção ao dispositivo é realizada anualmente, a não ser que seja lançado atualizações de segurança\falhas ou que o dispositivo apresente erros reportados pelo utilizador.

### 3.17 Direitos de autor

Os utilizadores não devem fazer cópias de software, propriedade da organização, exceto nos casos permitidos por lei, pelo proprietário.

Os utilizadores não devem copiar software ou outros materiais originais de outras fontes e são responsáveis por todas as consequências que possam surgir sob a lei de propriedade intelectual.

## 4. RESTRIÇÕES SOBRE A INSTALAÇÃO DE SOFTWARE

O software adicional que não esta na lista programas autorizados deve ter aprovação pelo responsável da área para depois proceder a instalação com a ajuda do departamento TI.

## 5. SEGREGAÇÃO DAS REDES

A rede interna esta dividida em 4 vlan’s que separara o sistema da central telefónica, as antenas dos telefones sem fios, a rede interna e o WiFi convidado. Essa separação melhora a segurança e a comunicação entre equipamentos.

## 6. POLÍTICA DE TRANSFERENCIA

A política de transferência esta referenciado no modelo IT 22.19 - Política de transferência.

## 7. ACORDOS DE CONFIDENCIALIDADE

São estabelecidos acordos de confidencialidade nas relações contratuais com clientes e fornecedores.

## 8. REGISTO DE INCIDENTES

Os incidentes reportados são recebidos no e-mail suporte ou via telefone. O técnico de informática que recebe o incidente regista no software Spicework – Helpdesk e é atribuído um número do incidente.

O incidente é depois atribuído ao técnico que vai resolver o problema identificado pelo utilizador.

## 9. REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta política é revista anualmente no momento de Revisão Pela Gestão de acordo com PG1

As alterações à política são controladas de acordo com o PG6 Controlo de Documentos.