## Introdução

A Política de Segurança da Informação (PSI) é um conjunto de diretrizes e práticas destinadas a proteger dados e sistemas contra ameaças, garantindo confidencialidade, integridade e disponibilidade das informações.

No Brasil, a Política Nacional de Segurança da Informação (PNSI) foi instituída pelo Decreto nº 9.637/2018 e abrange segurança cibernética, defesa cibernética, proteção de dados e segurança física. Ela é implementada por meio da Estratégia Nacional de Segurança da Informação (ENSI), que define ações estratégicas para fortalecer a segurança digital.

## 1. Objetivo

Esta política tem como objetivo descrever como a ÓGUI, garante a recepção, tratamento de dados e segurança da informação no escopo de sua atuação, atendendo aos requisitos da Lei Geral de Proteção de Dados Pessoais, a Lei 13.709/2018, ou LGPD. Define responsabilidades e orienta a conduta dos usuários da empresa, visando a continuidade dos negócios através da confidencialidade, da integridade e da disponibilidade das informações pela ÓGUI. Essas diretrizes tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade das informações dos clientes e internas.

## 2. Responsabilidades

Pessoas sócias, pessoas colaboradoras, estagiárias e fornecedores da ÓGUI, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvam a instituição.

### 2.1 Definições

A lei Nº 13.709, também conhecida como Lei Geral de Proteção de Dados, faz a distinção de dois agentes de dados: Operador e Controlador de dados.

Para fins legais, a ÓGUI é considerada como o ***Controlador*** dos dados, assim como cada uma das sócias em sua pessoalidade. Da mesma forma, cada pessoa colaboradora, fornecedor ou especialista contratado pode ser entendido como ***Operador*** dos dados. Além disso, ***Agentes de Tratamento de Dados*** são as pessoas (naturais ou jurídicas, de direito público ou privado) responsáveis por realizar qualquer atividade que envolva o uso de dados pessoais

**2.2 Sanções e Penalidades**

É de inteira responsabilidade do Operador qualquer prejuízo ou dano sofrido ou causado a ÓGUI e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.

As sanções abaixo serão aplicadas à pessoa colaboradora e especialistas que, após comprovação por meio de investigação, tiverem descumprido ou não seguido as disposições da Política de Segurança da Informação da ÓGUI Consultoria.

A medida tomada será baseada na gravidade da conduta e na eventual reincidência do ato:

- Advertência oral;
- Advertência escrita;
- Suspensão de 1 à 29 dias conforme gravidade;
- Demissão por Justa Causa.
- Se pessoa jurídica, rescisão imediata do contrato, desobrigando a ÓGUI a notificar com antecedência a data de término e consequentemente desobrigando o pagamento de multa por rescisão antecipada.

Se a conduta extrapolar a área trabalhista, serão executadas as medidas legais previstas na lei Nº 13.709.

De acordo com o Art. 52 “Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - Eliminação dos dados pessoais a que se refere a infração;

**2.3 Boas Práticas**

Cabe a todos os usuários as seguintes práticas:

• Cumprir fielmente políticas, normas e procedimentos de Segurança da Informação, incluindo regras estabelecidas neste documento;

• Buscar orientação da pessoa superiora quando houver dúvidas relacionadas à Segurança da Informação;

• Assinar o Termo de Responsabilidade, formalizando a ciência da PSI e das Normas de Segurança da Informação,

• Proteger as informações contra o acesso, a modificação, a divulgação ou a destruição não autorizada pela ÓGUI;

• Assegurar que os recursos tecnológicos utilizados sejam utilizados apenas para fins profissionais durante o horário de expediente aprovados e de interesse da instituição;

• Prezar pela segurança das informações confidenciais dos clientes, incluindo todo e quaisquer dados pessoais a que tiverem acesso;

• Atender à LGPD, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade às regras da ÓGUI.

- Comunicar imediatamente à pessoa gestora sobre qualquer descumprimento ou violação da PSI e/ou de suas Normas e Procedimentos, quando se tratar de infrações administrativas causadas por pessoas sócias, funcionárias, estagiárias e fornecedores da ÓGUI.

## 3. Requisitos da Política de Segurança

A PSI da ÓGUI deve ser comunicada a todos os funcionários, prestadores de serviço externos, estagiários e todos que compõem o ecossistema da empresa. Sempre que houver a contratação de um funcionário ou fornecedor, esta Política deve ser apresentada e lida pelo novo contratado para ciência.

O uso do Sharepoint, Teams e e-mail só poderão ser acessados após formalizarem a ciência sobre a PSI. Este processo deve ser formalizado e incluído durante a fase de contratação e inclusa nos contratos de prestação de serviço.

## 4. Classificação de dados

Considerando toda operação da ÓGUI, podemos classificar os dados da seguinte forma:

### 4.1 Informações Confidenciais

As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da empresa. Exemplos: Planejamento Estratégico completo; Controles internos; e afins.

### 4.2 Informações Restritas

É o nível médio de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores. São protegidas, restringindo o acesso a uma pasta ou diretório da rede. Exemplos: Documentos relacionados a gestão de Pessoas; Registros de

Avaliação de Desempenho de pessoas colaboradoras; Fluxo de Caixa e Controles Financeiros e Contábeis; Propostas Comerciais; Painel completo de KPIs; Descrição da Metodologia e ferramentas do atendimento e afins.

### 4.3 Informações de Uso Interno

São informações de clientes e da ÓGUI que não podem ser publicadas externamente. Estas informações devem ser armazenadas apenas dentro do ambiente do SharePoint, o compartilhamento externo deve ser feito com o cliente em questão. No caso de informações institucionais dos clientes, o acesso deve ser feito com a autorização da gestão, vale para informações de processos ÓGUI. Exemplos: Drafts de apresentação de resultados; Planilhas e ferramentas desenvolvidas para aplicar as consultorias; Ferramentas de planejamento de projetos...

### 4.4 Informações Públicas

São informações que são de domínio público ou que não existe risco em compartilhamento externo. Exemplos: Relatórios de Sustentabilidade publicados pelos clientes; Apresentações institucionais; ...

### 4.5 Informações Pessoais:

Ou dados pessoais, são quaisquer informações sobre um indivíduo identificado ou a partir dos quais uma pessoa única possa ser identificada. Exemplos: Dados de contato, como nome completo, telefone, e-mail, endereço e data de nascimento; Dados profissionais, como cargo e empresa onde o titular trabalha e dados presentes em currículos (como formação, histórico de empregos e qualificações profissionais); Dados publicados pelo titular em redes sociais; Dados pessoais sensíveis como classe social, deficiências físicas, orientação sexual e religiosa e origem racial ou étnica de alguns grupos de titulares em projetos de inclusão e diversidade.

## 5. Ferramentas tecnológicas para gestão da informação

### 5.1 *Office* 365

O Office 365 é uma suíte de produtividade baseada em nuvem da Microsoft oferece uma variedade de ferramentas e serviços para ajudar as organizações a trabalhar de forma mais eficiente e colaborativa.

O pacote contratado pela ÓGUI, para todas as pessoas colaboradoras contratadas e estagiários inclui aplicativos populares como Word, Excel, PowerPoint, Outlook e Teams, além de serviços de armazenamento em nuvem e compartilhamento de arquivos.

### 5.2 Servidor

Além disso, por motivos de segurança, existe um servidor físico na sede da ÓGUI para realização de backups de segurança. A rotina de backup é definida de acordo com o tópico 9.

A gestão das informações inseridas neste servidor é de responsabilidade do Analista Administrativo Financeira. Periodicamente, as informações nele contidos, são revisadas e restauradas mediante solicitação da operação. O intuito chave deste Servidor é salvaguardar as entregas e o capital intelectual da ÓGUI ao longo dos anos.

### 5.3. Recursos de Whatsapp

Para comunicações rápidas com os clientes, usamos a ferramenta whatsapp. Atualmente, o Whatsapp usado é o número pessoal do funcionário. Desta forma, deve ser redobrada a atenção para o uso da ferramenta e as interações com os clientes apenas durante o horário de expediente.

## 6. Gestão no ambiente da *Microsoft*

### 6.1 Introdução

Para detalhar a aplicação prática dessas permissões e garantir a rastreabilidade das responsabilidades, será elaborado uma Norma específica. Este documento apresentará uma tabela clara e concisa das permissões de acesso no ambiente *Microsoft 365*, juntamente com a identificação dos indivíduos ou grupos responsáveis por sua atribuição e manutenção. Esta Política será submetida a uma revisão anual, assegurando que as permissões estejam sempre alinhadas com as necessidades da organização e as melhores práticas de segurança.

Seguimos os tipos de acesso e permissões detalhados na página do Centro de Administração do *Microsoft 365*. Além disso, estruturamos toda arquitetura de acesso na Norma_Tipos de Permissão e Acesso.

### 6.2 Tipos de Permissão e Acesso

Com relação aos tipos de acesso e permissões do ambiente Microsoft:

1. Administrador Global – Acesso total ao ambiente, pode gerenciar todos os serviços e usuários.

2. Administrador de Usuário – Gerencia usuários e grupos, pode redefinir senhas e atribuir funções.

3. Administrador de Cobrança – Gerencia faturas, pagamentos e assinaturas.

4. Administrador do Exchange – Gerencia e-mails, caixas postais e políticas do Exchange Online.

5. Administrador do SharePoint – Controle sobre sites, permissões e compartilhamentos no SharePoint Online.

6. Administrador do Teams – Gerencia políticas, configurações e permissões do Microsoft Teams.

7. Administrador de Suporte – Abre e gerencia chamados de suporte junto à Microsoft.

8. Administrador de Segurança – Gerencia políticas de segurança, auditorias e conformidade.

9. Administrador de Conformidade – Gerencia políticas de conformidade, DLP (Prevenção contra perda de dados) e auditorias.

### 6.3 Orientações Gerais

Os recursos de TI alocados pela ÓGUI aos seus usuários são destinados exclusivamente às atividades relacionadas ao trabalho, sendo proibido o uso dos mesmos com para fins pessoais.

Com relação a pessoa colaboradora, atualmente se usa equipamento próprio para o trabalho, porém, é proibido o uso de computadores, tablet ou modificação, bem como a transferência e/ou a divulgação de qualquer software, programa ou instruções, notebooks, *netbooks* e similares que não sejam devidamente avaliados pela equipe de TI e do Administrativo Financeiro.

É proibido o uso de software de e-mail, mensagens instantâneas e correio interno não homologado pela Direção e são de responsabilidade do usuário e podem trazer riscos à segurança da informação além de dificultar o suporte técnico.

## 7. Autenticação e autorização de uso do ambiente da Microsoft

### 7.1 Autenticação

O processo de verificação da identidade de um usuário antes de permitir o acesso aos recursos e dados da empresa deve ser feito com cautela. Para isso todos os usuários devem utilizar senhas fortes e únicas para acessar os recursos e dados da empresa.

Com relação a continuar conectado, precisa-se **atentar para não manter sua conta ÓGUI conectada em um computador ou celular que não seja o seu.**

### 7.2 Autorização

O processo de verificação se um usuário tem permissão para acessar um recurso ou dado específico. A ÓGUI atribui permissões específicas a cada usuário para acessar recursos e dados. Cada tipo de acesso é determinado. Dessa forma, a ÓGUI possui grupos de segurança que definem o seu nível de acesso, tais como:

1. Acesso SÓCIAS;
2. Acesso Gestão Financeiro/RH;
3. Acesso Gestão Clientes/Comercial;
4. Acesso Padrão Produção.

## 8. Armazenamento de arquivos

Todos os arquivos contidos nos servidores de rede devem ser exclusivamente de interesse da ÓGUI.

- É proibida a criação de pastas pessoais nos servidores de rede.
- A criação de pastas departamentais nos servidores de rede deverá refletir a estrutura organizacional da ÓGUI e ser autorizada pelo responsável hierárquico.
- O acesso às pastas departamentais nos servidores de rede exige autorização do responsável hierárquico para o controle do acesso de cada usuário.
- Todos os arquivos que sejam relacionados a operação da ÓGUI deverão ser excluídos do seu servidor pessoal para evitar problemas futuros com as auditorias.
- Os usuários devem manter obrigatoriamente os arquivos, planilhas, e-mails, apresentações, desenhos, e outros dados críticos da ÓGUI, nas pastas departamentais do servidor de rede.

## 9. Salvaguardas, Backups e recuperação de dados

Para a realização de backups, é responsabilidade do Analista Administrativo/Financeira a realização periódica de backups de histórico de clientes e dados institucionais da ÓGUI no servidor físico disponível. Compete ao Analista Administrativo Financeira criar e manter cópias de segurança (backups) apenas dos dados armazenados nos servidores de rede;

Para realização deste backup, o deve ser feito o salvamento dessas informações, priorizando as informações ***Superadas*** e de ***Clientes Inativos.*** Além disso, deve-se

realizar o backup sempre que o armazenamento chegar a um **nível crítico (+90%).** O processo detalhado de Backup será detalhado no POP_Backup e Recuperação de Dados.

# 10. Gestão de Dados Pessoais

## 10.1 Definição de Dados Pessoais

Dados pessoais referem-se a informações que identificam ou podem identificar um indivíduo, seja ele um cliente, funcionário, parceiro ou qualquer outra pessoa que tenha relação com a ÓGUI ou algum de seus clientes. Dessa forma, Dados Pessoais podem ser classificados como:

- Dados pessoais de colaboradores;
- Dados pessoais de fornecedores;
- Nome, telefone e e-mail de Stakeholders;
- Dados pessoais do responsável legal do cliente

## 10.2 Tratamento de Dados Pessoais

Usando como base o Artigo 5 da Lei Geral de Proteção de dados, entende-se como Tratamento de Dados “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

Dessa forma, a ÓGUI entende que todas as suas operações, dependem do tratamento desses dados, sejam de clientes, sejam de seus colaboradores (para fins de gestão interna). O cumprimento da legislação se baseia no Artigo 7, considerando duas hipóteses para o tratamento desses dados:

1. “para o cumprimento de obrigação legal ou regulatória pelo controlador (ÓGUI)” (Colaboradores);
2. “quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (Clientes);

## 10.3 Guarda e Acesso de Dados Pessoais

Com relação a Legislação, a LGPD não especifica o prazo pelo qual os dados podem ser armazenados e tratados. Todos os dados de Colaboradores, Ex Colaboradores, Fornecedores e ex Fornecedores devem ser classificados como Dados Confidenciais e armazenados considerando possíveis obrigações legais futuras.

Sobre os dados de Stakeholders, devem receber o mesmo tratamento dos Dados Confidenciais Restritos de Uso Interno, que serão descritos no próximo tópico.

## 11. Tratamento de Dados Confidenciais Restritos de Uso Interno

Sobre Informações Institucionais de Clientes, deve-se ter os seguintes procedimentos:

- Local: Todos os documentos institucionais enviados pelo cliente devem armazenados exclusivamente na pasta compartilhada do cliente (Clientes)
- O arquivamento de documentos institucionais fora do ambiente do Sharepoint é **terminantemente proibido**.
- Compartilhamento com fornecedores externos: O compartilhamento de dados ou execução com fornecedores externos deve ser feita apenas após a assinatura do NDA;
- Período de armazenamento: 6 meses após o fim do atendimento.

## 12. Segurança de sistemas

### 12.1 Antivírus

A ÓGUI, visando proteger seu ambiente contra ameaças, disponibiliza e mantém atualizado, um software antivírus corporativo em todos os computadores de trabalho. Este antivírus é atualizado automaticamente, garantindo que cada usuário se beneficie das últimas proteções assim que disponibilizadas pelo fabricante. É recomendado que os usuários não removam ou alterem as configurações deste software, a fim de preservar a integridade da segurança proporcionada.

### 12.2 Softwares Adjacentes

Além disso, todos os softwares homologados e instalados nos computadores e servidores da rede são de propriedade exclusiva da ÓGUI, sendo estritamente proibida qualquer forma de cópia, integral ou parcial, bem como a instalação de

softwares não autorizados ou piratas. A pirataria, além de ser considerada crime com as penalidades legais cabíveis de detenção e multa conforme a Lei nº 9.609/98, expõe a organização a riscos significativos, incluindo prejuízos materiais, falhas funcionais e danos à imagem institucional, sendo, portanto, terminantemente proibida em todos os seus âmbitos.

**12.3 Processo de Segurança**

A ÓGUI utiliza a solução de criptografia nativa da plataforma Microsoft 365 para proteção de suas informações confidenciais, inclusive de dados protegidos pela LGPD.

## 13. Monitoramento e auditoria

A ÓGUI busca implantar um sistema de monitoramento e auditoria para garantir a segurança, a integridade e a disponibilidade de seus ativos de informação e de seus clientes.

O monitoramento contínuo tem como objetivo identificar e responder proativamente a incidentes de segurança, vulnerabilidades, acessos não autorizados e desvios de políticas. As informações coletadas são analisadas para detectar padrões suspeitos, anomalias e potenciais ameaças, permitindo ações corretivas imediatas e aprimoramento contínuo dos controles de segurança.

Auditorias de segurança da informação serão conduzidas ***semestralmente*** pelo *Analista Administrativo Financeira* para avaliar a eficácia dos controles implementados, a conformidade com esta política e com as regulamentações aplicáveis. Os resultados das auditorias serão documentados e utilizados para identificar oportunidades de melhoria e fortalecer a postura de segurança da ÓGUI.

As etapas da auditoria serão:

- **Revisão de políticas e procedimentos:** Analisar a documentação existente relacionada à segurança do SharePoint, como procedimentos de gerenciamento de permissões, planos de resposta a incidentes;
- **Análise de configurações do SharePoint:** Verificar as configurações de segurança do sistema, incluindo autenticação, autorização, configurações de auditoria, políticas de segurança de conteúdo;

- **Análise de permissões:** Avaliar as permissões de acesso a sites, listas, bibliotecas, documentos e outros objetos do SharePoint para garantir o princípio do menor privilégio;
- **Entrevistas com pessoal chave:** Conversar com administradores do SharePoint, proprietários de sites e usuários para entender os processos de segurança e identificar possíveis preocupações;
- **Testes de segurança:** Realizar testes de penetração ou análise de vulnerabilidades para identificar falhas de segurança exploráveis (geralmente realizado por especialistas em segurança);

Serão mantidos registros detalhados das atividades de monitoramento e auditoria, incluindo logs de acesso, alterações de configuração, alertas de segurança e ações de resposta a incidentes, em conformidade com os requisitos legais e regulatórios. O acesso a esses registros será restrito e controlado, garantindo a sua confidencialidade e integridade.

A ÓGUI compromete-se a investir continuamente em ferramentas e tecnologias de monitoramento e auditoria, bem como na capacitação de seus colaboradores, para assegurar a efetividade deste tópico e a proteção de seus ativos de informação.

## 14. APROVAÇÃO

| Responsável (Ordem Alfabética) | Cargo | Data e Assinatura |
|---|---|---|
| **Andreia Amorim** | Diretora de Estratégia e Gestão | ANDREIA SILVA DA ROSA DE AMORIM:00438450965 Assinado de forma digital por ANDREIA SILVA DA ROSA DE AMORIM:00438450965 Dados: 2026.02.24 18:16:49 -03'00' |
| **Estela Kurth** | Diretora de Divulgações ESG | ESTELA DORIS KURTH:55129374991 Assinado digitalmente por ESTELA DORIS KURTH:55129374991 ND: C=BR, CN=ESTELA DORIS KURTH:55129374991, O=ICP-Brasil, OU=14121957000109 Razão: Eu sou o autor deste documento Localização: Data: 2026.02.19 09:18:53-03'00' Foxit PDF Reader Versão: 2025.3.0 |
| **Velma Gregório** | CEO | SIGNATÁRIO Velma De G. C. Pereira Data 25/02/2026 10:40 #b3d8d25d124511f1bb8342010a2b6020 |

| Aprovação | Data 25.07.2025 |
|---|---|
| Aprovação do documento | |
| 1º alteração | |
| 2º alteração | |
| 3º alteração | |