

POLÍTICA DE CONFIDENCIALIDADE

Responsável: Segurança da Informação

Classificação: Interna

Versão: 1

Identificador: PSI 04

ÍNDICE

1.	INTRODUÇÃO.....	3
2.	DEFINIÇÕES.....	3
3.	OBJETIVO.....	4
4.	ABRANGÊNCIA.....	4
4.1.	ISENÇÕES.....	4
5.	REQUISITOS DE CONFIDENCIALIDADE.....	4
5.1.	DETENTORES DE INFORMAÇÕES PRIVILEGIADAS.....	5
6.	RESPONSABILIDADES.....	5
6.1.	CONGLOMERADO PRUDENCIAL GENIAL.....	5
6.2.	DIRETOR DE TECNOLOGIA, RISCO E COMPLIANCE.....	6
6.3.	COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI).....	Erro! Indicador não definido.
6.4.	GERENCIA DE SEGURANÇA DA INFORMAÇÃO.....	6
6.5.	GESTORES DA INFORMAÇÃO.....	7
6.6.	COMPLIANCE.....	Erro! Indicador não definido.
6.7.	RECURSOS HUMANOS.....	7
6.8.	USUÁRIOS DA INFORMAÇÃO.....	7
6.9.	PRESTADORES DE SERVIÇO.....	8
7.	VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.....	8
8.	DOCUMENTOS RELACIONADOS.....	8
9.	VIGÊNCIA.....	9
10.	CONTROLE DE VERSÕES.....	9

1. INTRODUÇÃO

A guarda e a movimentação de informações confidenciais, seja na forma física (registros em papel) ou eletrônica (e-mails ou outros meios eletrônicos) podem representar um risco para o Conglomerado Prudencial Genial ("Conglomerado"; "Grupo Genial") se inadequadamente protegidos. Assim, todos os seus sócios, administradores, colaboradores e terceiros contratados são pessoalmente responsáveis por assegurar que dados confidenciais (aqueles não públicos, protegidos ou não por acordos de confidencialidade) relacionados a clientes, provedores, contrapartes, outros colaboradores, estratégias de negócios ou relacionado a qualquer outro terceiro que mantenha uma relação de negócios com o Grupo Genial sejam mantidos em segurança.

2. DEFINIÇÕES

Termos	Definições
CONFIDENCIALIDADE	É a garantia que todos os meios de processamento e/ou conservação de informação contenham medidas de proteção quanto ao acesso e utilização por pessoa não-autorizada, assegurando que toda informação esteja protegida de revelações acidentais, espionagem industrial, violação da privacidade e outras ações similares.
INTEGRIDADE	É a garantia que todas as informações processadas, transacionadas ou armazenadas nas bases e sistemas do Conglomerado Prudencial Genial estejam livres de erros e irregularidades de qualquer espécie, assegurando que toda informação processada em cada um dos sistemas de informação e processos transacionais seja necessária, útil e suficiente para o desenvolvimento dos negócios.
DISPONIBILIDADE	É a garantia que a informação e sua capacidade de processamento, manual ou automática, sejam resguardadas e recuperadas sempre que necessário, de modo a não impactar significativamente o andamento dos negócios, estando sempre ao dispor da entidade que a solicitar.
CONFORMIDADE/COMPLIANCE	É a garantia que toda informação e os meios físicos que a contenham, processem e ou transportem, cumpram com os regulamentos legais vigentes em cada âmbito, e que todos os direitos de propriedade sobre a informação utilizada ou produzida pelo Conglomerado Prudencial Genial, no desenvolvimento de suas atividades, estejam adequadamente estabelecidos a favor da empresa.
PRIVACIDADE	É a garantia que toda informação que pode potencialmente identificar um indivíduo relacionado com o Conglomerado Prudencial Genial seja coletada, armazenada, processada, compartilhada e descartada de forma segura.
ATIVO	É tudo aquilo que o Conglomerado Prudencial Genial considerar como relevante para o negócio, desde ativos tecnológicos (p.ex.: hardware, software), até não tecnológicos (p.ex.: pessoas, processos, dependências físicas), desde que estejam relacionados à proteção da informação.
RISCO	É a probabilidade de um agente de ameaça explorar uma vulnerabilidade em qualquer ativo, dessa forma quebrando um ou mais princípios da

	confidencialidade, integridade, disponibilidade ou conformidade, assim gerando prejuízos ao Conglomerado Prudencial Genial.
--	---

3. OBJETIVO

Essa política tem por objetivo estabelecer os conceitos e diretrizes de confidencialidade no Conglomerado, assim como estabelecer boas práticas das informações visando garantir uma relação de confiança, respeito e transparência com seu público.

4. ABRANGÊNCIA

Esta política é aplicada às instituições do Conglomerado e seus sócios, administradores, colaboradores e terceiros contratados, , partes interessadas que possam tratar ou transmitir dados e/ou informações, assim como qualquer recurso intelectual de propriedade do Grupo.

4.1. ISENÇÕES

Qualquer exceção ou isenção desta política deve antes ser aprovada pelo Comitê de Segurança da Informação.

5. REQUISITOS DE CONFIDENCIALIDADE

- Todos os colaboradores e terceiros envolvidos nos serviços financeiros devem exercer a máxima discrição no trato das informações sensíveis. Estas informações incluem, mas não estão limitadas a, dados de clientes, estratégias de investimento, planos de negócios, informações de fusões e aquisições, bem como outros dados que possam impactar a segurança financeira, de imagem, regulatória da empresa ou de seus clientes.
- O acesso às informações privilegiadas deve ser restrito apenas aos colaboradores que possuem necessidade de conhecimento para o desempenho de funções específicas. O Grupo Genial garante sistemas de controle de acesso, para que apenas os indivíduos autorizados tenham permissão para acessar informações, neles contidas.
- Qualquer compartilhamento de informações privilegiadas com terceiros deve ser devidamente autorizado pelo Grupo Genial e formalizado por meio de acordos de confidencialidade. Os colaboradores são instruídos a cumprir rigorosamente os termos desses acordos, garantindo que as informações permaneçam sob sigilo.
- Cada colaborador deve reconhecer sua responsabilidade individual no tratamento das informações confidenciais. É imperativo que todos os funcionários entendam que são proibidos de utilizar

informações privilegiadas em benefício próprio ou de terceiros, bem como de divulgar tais informações, mesmo após o término do vínculo empregatício.

- O Grupo Genial fornece treinamentos adequados sobre a política de confidencialidade a todos os colaboradores e terceiros que tenham acesso a informações sensíveis. Além disso, promove uma cultura de conscientização sobre a importância da confidencialidade em todas as operações relacionadas aos serviços financeiros.
- O Grupo Genial estabelece mecanismos de monitoramento e auditoria para garantir o cumprimento da política de confidencialidade. Isso pode incluir a revisão regular dos registros de acesso, a condução de auditorias internas e a implementação de medidas corretivas, se necessário.
- O Grupo Genial desenvolveu e mantém uma política de segurança da informação e cibernética que detalha os testes periódicos de segurança para os sistemas de informações confidenciais, especialmente para os mantidos em meio eletrônico.

5.1. DETENTORES DE INFORMAÇÕES PRIVILEGIADAS

Os detentores de informações privilegiadas, com base em seus cargos ou atribuições, a fim de estabelecer uma clara barreira de informações com os demais funcionários são:

- **Alta Administração:** Membros da Diretoria Executiva e demais diretores.
- **Áreas Financeiras:** Colaboradores diretamente envolvidos em operações financeiras, Contabilidade, Tesouraria e Análise de Investimentos.
- **Compliance, Riscos e Jurídico:** Membros com acesso a informações sobre regulamentações, investigações, litígios e assuntos jurídicos confidenciais da empresa.

6. RESPONSABILIDADES

Todas as informações geradas e manuseadas pelos colaboradores e parceiros, no exercício de sua função, são de propriedade do Conglomerado, portanto, devem ser manuseadas da forma correta, assegurando sua proteção, de forma a respeitar suas diretrizes de confidencialidade e classificação.

6.1. CONGLOMERADO PRUDENCIAL GENIAL

É dever do Conglomerado :

- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: sócios, administradores, colaboradores e terceiros contratados;
- Elaborar, implantar e seguir as políticas, normas e procedimentos de Segurança da Informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação sejam atendidos através da adoção de controles contra ameaças provenientes de fontes internas ou externas;

- Garantir a educação e conscientização sobre as práticas adotadas pelo Conglomerado de confidencialidade para seus sócios, administradores, colaboradores e terceiros contratados;
- Atender os requisitos de confidencialidade de regulamentações, leis e/ou cláusulas contratuais.

6.2. DIRETORIA DE TECNOLOGIA

É responsabilidade da Diretoria de Tecnologia

- Promover os recursos necessários para a implantação de controles tecnológicos; e de Segurança; da Informação
- Assegurar a efetividade e o cumprimento das diretrizes desta e demais políticas, relacionadas à Tecnologia e Segurança da Informação, pelos sócios, administradores, colaboradores e terceiros contratados;
- Atestar o cumprimento das legislações e regulamentações vigentes, no que tange os recursos tecnológicos e segurança da informação.

6.3. DIRETORIA DE RISCO E COMPLIANCE

É responsabilidade da Diretoria de Risco e Compliance

- ;
- Garantir a efetividade dos meios de comunicação para a disseminação desta e demais normas e políticas relacionadas à segurança da informação;
- Assegurar a efetividade e o cumprimento das diretrizes desta e demais políticas, relacionadas à Confidencialidade, Segurança da Informação do Grupo Genial;
- Garantir o cumprimento das legislações e regulamentações vigentes, no que tange a confidencialidade e segurança da informação do Conglomerado.

6.4. SEGURANÇA DA INFORMAÇÃO

É responsabilidade da área de Segurança da Informação:

- Garantir os recursos necessários para a implementação de controles de confidencialidade;

- Conduzir a gestão e a operação da Segurança da Informação, tendo como base essa política e as demais normas publicadas;
- Apoiar o Comitê de Segurança da Informação ("Comitê") em suas deliberações;
- Elaborar e propor ao Comitê as normas e procedimentos de segurança da informação, necessários para se fazer cumprir esta política;
- Identificar e avaliar as principais ameaças à confidencialidade dos dados e informações, bem como propor e implantar medidas corretivas para reduzir os riscos.

6.5. GESTORES DA INFORMAÇÃO

É responsabilidade dos Gestores da Informação:

- Gerenciar as informações geradas, ou sob a responsabilidade da sua área de negócio, durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte, conforme as normas estabelecidas pelo Conglomerado;
- Identificar, classificar e rotular as informações geradas, ou sob responsabilidade da área de negócio, conforme normas, critérios e procedimentos adotados pela companhia;
- Revisar e autorizar os acessos à informação e sistemas sob sua responsabilidade;
- Solicitar a concessão ou a revogação de acesso a informação ou sistemas, de acordo com a norma adotada pelo Conglomerado;
- Informar para a área de Recursos Humanos qualquer transferência de cargo ou desligamento de qualquer colaborador sob sua gestão;
- Solicitar o imediato cancelamento do acesso aos ativos de TI de todo o colaborador, sob a sua gestão, que seja desligado ou transferido de função;

6.6. RECURSOS HUMANOS

É responsabilidade dos Recursos Humanos:

- Informar aos Gestores da Informação, qualquer movimentação, envolvendo transferências e desligamentos, dos colaboradores sob sua gestão;
- Estabelecer os controles de confidencialidade específicos para os processos de contratação, desligamento e modificação das atividades dos colaboradores.
- Disponibilizar e assegurar o cumprimento da Política de Confidencialidade para todos os colaboradores, do Conglomerado.

6.7. USUÁRIOS DA INFORMAÇÃO

É responsabilidade dos Usuários da Informação:

- Ler, compreender e cumprir integralmente os termos da Política de Confidencialidade, bem como as demais normas e procedimentos de segurança aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre esta política, normas e procedimentos para o endereço de e-mail da área de Segurança da Informação: **ol.si.governanca@genial.com.vc**;
- Comunicar para a área de Segurança da Informação qualquer evento que viole esta política ou que possa vir a colocar em risco a confidencialidade das informações e/ou recursos computacionais do Conglomerado Prudencial Genial para o endereço de e-mail: **csirt@genial.com.vc**.
- Utilizar os ativos de TI única e exclusivamente para os fins a que foram destinados e de interesse do Conglomerado;
- Responder pela inobservância da Política de Confidencialidade, normas e procedimentos de segurança, conforme definido no item **Violação da Política da de Segurança da Informação**;
- Respeitar o caráter confidencial das senhas de acesso aos ativos de TI que lhe forem concedidas;

6.8. PRESTADORES DE SERVIÇO

É responsabilidade dos Prestadores de Serviço:

- Cumprir todo o conteúdo disposto nas Políticas, Normas e Procedimentos do Conglomerado; .

7. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como das demais normas e procedimentos de Segurança, serão passíveis de procedimentos disciplinares considerados como falta grave, conforme disposto no **Código de Ética e Conduta** do Conglomerado Prudencial Genial, ou de acordo com análise de decisão do Comitê de Segurança da Informação, sujeitando o colaborador a sanções administrativas de acordo com o grau de severidade do incidente.

No caso de terceiros contratados ou prestadores de serviço, o Comitê deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

8. DOCUMENTOS RELACIONADOS

Esta política é complementada por normas, procedimentos, manuais, programas de conscientização e relatórios específicos de Segurança da Informação em conformidade com os aspectos legais e com base nos seguintes documentos:

- NOR SI 08 – Segurança para Uso Aceitável
- NOR SI-09 – Segurança para Classificação e Tratamento Informação
- NOR SI 17 – Gestão de Riscos de Segurança da Informação
- POL SI 01 – Política de Segurança da Informação e Cibernética
- POL SI 02 – Segurança da Informação para Terceiros
- PMTL 01 – Política de Mesa e Tela Limpa
- Código de Ética e Conduta
- Manual de Gerenciamento de Risco Operacional
- Manual de Gestão de Barreiras e Informação;
- Política de Privacidade

9. VIGÊNCIA

Esta política possui prazo de vigência de um ano a partir da data de sua publicação ou conforme o entendimento do Comitê de Segurança da Informação.

10. CONTROLE DE VERSÕES

Data	Versão	Descrição	Autor
27.07.2023	01	Criação do Documento	Segurança da Informação



genialinvestimentos.com.br