



	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	1 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022


<p>Política de Segurança da Informação – Versão Pública</p>	<p><i>Information Security Policy – Public Version</i></p>
--	---



	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	1 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	2 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

Sumário | Summary:

1.	Introdução	3
1.	Introduction	3
2.	Objetivo	3
2.	Objective	3
3.	Abrangência / Áreas Envolvidas.....	4
3.	Scope / Areas Involved	4
4.	Princípios.....	4
4.	Principles.....	4
5.	Diretrizes Gerais	5
5.	General Guidelines.....	5
6.	Legislação / Regulação Relacionada.....	9
6.	Legislation / Regulation Related.....	9

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	2 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	3 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

1. Introdução

A hEDGEpoint Global Markets (“HPGM” ou “Grupo HPGM”) reconhece a importância da Segurança da Informação (SI), como meio para o cumprimento de sua missão, valores e estratégia de negócio, assim como investe constantemente no crescimento profissional de seus colaboradores e em tecnologias que garantam a qualidade e segurança de seus produtos e serviços.

Esta Política de Segurança da Informação (PSI) foi elaborada para garantir a sua aderência às Legislações vigente.

2. Objetivo

A PSI é o documento que expressa o posicionamento do Grupo HPGM em relação à proteção e preservação dos seus ativos (informação, dados e equipamentos tecnológicos) e tem como objetivo:

- I. Declarar formalmente o comprometimento da Alta Direção do Grupo HPGM, na promoção de diretrizes estratégicas, responsabilidades, competências e apoio ao Sistema de Gestão de Segurança da Informação (SGSI), a fim de garantir a proteção dos seus ativos tangíveis e intangíveis;
- II. Estabelecer as responsabilidades e os limites de atuação dos colaboradores do Grupo HPGM em relação à SI, reforçando a cultura interna e priorizando as ações necessárias conforme negócio;

1. Introduction

hEDGEpoint Global Markets (“HPGM” or “HPGM Group) recognizes the importance of Information Security (IS) to the fulfillment of its mission, values, and strategy of the business, as well as the result of constant investment in the professional development of its employees and technology, to ensure the quality and safety of our products and services.



This Information Security Policy (ISP) has been developed to ensure adherence to the Laws in force.

2. Objective

The ISP expresses the position of HPGM Group concerning the protection and preservation of its assets (information, data, and hardware) and it has the following objectives:

- I. Declare a formal commitment from the Executive Management of the HPGM Group to the promotion of the strategic framework, responsibilities, skills, and support to the Information Security Management System (ISMS) to ensure the protection of both tangible and intangible assets.*
- II. To establish responsibilities and boundaries of the HPGM Group employees concerning IS, reinforcing an internal culture and prioritizing the necessary actions according to the business.*

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	3 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	4 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

III. Viabilizar a confidencialidade, disponibilidade e integridade das informações e mitigar os riscos cibernéticos a um nível aceitável de acordo com o apetite de riscos estabelecido pela HPGM, definindo mecanismos e controles de proteção dos ativos de sua propriedade.

III. Enable the confidentiality, availability, and integrity of information and mitigate cyber risks to an acceptable level in accordance with the risk appetite established by HPGM, definition mechanisms, and controls for the protection of its assets.

3. Abrangência / Áreas Envolvidas

3. Scope / Areas Involved

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, estagiários, visitantes e prestadores de serviços que façam uso continuado ou eventual dos recursos tecnológicos do Grupo HPGM ou de sua rede de computadores.

This is an internal document with legal value and immediate and indistinct applicability, for the employees, interns, visitors, and service providers who make continuous or eventual use of the technological resources of HPGM Group including its computer network.

4. Princípios

4. Principles

Preservar e proteger as informações do Grupo HPGM ou sob sua reponsabilidade, em todo o seu ciclo de vida, contida em qualquer suporte ou formato, de vulnerabilidades e ameaças.

Preserve and protect the information of HPGM group or, any information under its responsibility, throughout its life cycle, contained in any media or format, from threats and vulnerabilities.



Prevenir e reduzir impactos gerados pelos incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades profissionais.

Prevent and reduce the impacts of information security incidents, ensuring confidentiality, integrity, availability, authenticity, and legitimacy in the development of professional activities.

Zelar por relações transparentes e éticas nos termos do Código de Conduta Ética e Integridade.

Maintain transparent and ethical relationships, following the Code of Ethical Conduct and Integrity.

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	4 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	5 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

Cumprir as legislações relacionadas ao negócio no que diz respeito à segurança da informação, assim como as legislações vigentes em cada país de atuação.

Comply with the industry related legislation regarding IS, including the laws in force in each country HPGM operates.

5. Diretrizes Gerais

5.General Guidelines

Interpretação: Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas nos normativos só devem ser realizadas após prévia e formal autorização do Gestor do colaborador.

Interpretation: *This ISP and its supporting documents shall be interpreted in a restrictive way, in other words, activities that are not comprised under HPGM's policies and procedures should only be performed after previous and formal consent from the employee's Manager.*

Propriedade: As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade do Grupo HPGM e devem ser utilizados unicamente para fins profissionais.

Property: *All information created, accessed, manipulated, stored, or disposed of, in the exercise of the activities carried out by our employees, as well as the rest of the intangible and tangible assets that are made available, is property of or under the responsibility of HPGM Group must be solely used for business purposes.*



Classificação da Informação: Todas as informações de propriedade ou sob a responsabilidade do Grupo HPGM devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida, conforme Política de Classificação da Informação.

Data Classification: *According to Data Classification Policy, all the information that is property of or under the responsibility of HPGM Group must be classified and protected with specific controls throughout its life cycle.*

Sigilo: É vedada, a qualquer tempo, a revelação de informação de propriedade ou sob a responsabilidade do Grupo HPGM sem a prévia e formal autorização do Gestor da Informação, excetuando-se a informação

Confidentiality: *It is not permitted, at any time, the disclosure of the information of property or under the responsibility of HPGM Group, without prior written formal permission from the Information Owner. Public*

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	5 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	6 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

pública. A informação é classificada como pública quando ela puder ser divulgada a todos, isto é, colaboradores, estagiários, visitante, prestadores de serviços e público em geral, sem que isso provoque impactos no negócio. Em caso de dúvida quanto a informação, procurar o Gestor imediato.

Uso dos Ativos: Os ativos de propriedade ou sob sua responsabilidade do Grupo HPGM devem ser utilizados somente para fins profissionais e de acordo com as orientações dos fabricantes e da empresa.

Controle de Acesso: A HPGM gerencia o acesso físico e lógico aos seus ambientes, ativos e informações. Desse modo, o colaborador recebe uma identidade digital de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

- I. O colaborador é responsável pelo uso, proteção e sigilo de sua identidade digital, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de suas credenciais, tal qual de terceiros.
- II. Para garantir o controle de acesso aos ambientes físicos e lógicos, a HPGM utiliza os critérios do mínimo conjunto necessário (*least privilege*) e estritamente necessários (*need to know*) ao definir os acessos de cada colaborador, conforme Política de Gestão de Acessos.



information is an exception to this rule. The information is classified as public when it can be disclosed to everyone (employees, interns, visitors, service providers, and the general public) with no impact on the business. Any question regarding data classification must be submitted to the line Manager.

Usage of Assets: *The assets owned or under HPGM Group's responsibility shall be used solely for business purposes and according to the manufacturer's and HPGM's guidelines.*

Access control: *The HPGM Group manages physical and logical access to its environments, assets, and information. Therefore, employees always receive a non-transferable and privately disclosed digital identity for personal use.*

- I. *The employee is responsible for the use, protection, and security of their digital identity, it is not allowed to share, give, save, replicate, publish or make any unauthorized use of his credentials including third parties.*
- II. *To ensure proper Physical and Logical environment Access Control, HPGM uses the criteria of "least privilege access" and "need to know access" to define access levels for each employee, according to Access Management Policy.*

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	6 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	7 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

Salvaguarda (backup): A HPGM mantém um processo de salvaguarda das informações e dos dados necessários para recuperação dos seus sistemas (backup), a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas, incidentes ou eventos disruptivos.

Monitoramento: A HPGM monitora seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio, a reputação e a identificação de eventos ou alertas de incidentes referentes à segurança da informação.

Gestão de Risco: O Departamento de Cybersecurity identifica e avalia os riscos relacionados à SI e Cibersegurança e adota as melhores práticas para o seu gerenciamento e controle.

Gestão de Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e na infraestrutura tecnológica do Grupo HPGM, devem preservar os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações e realizados somente pelo Departamento de TI.

Continuidade do Negócio: Os procedimentos de gestão de Continuidade do Negócio devem ser executados em

Comunicação de Incidentes: A HPGM possui um canal de comunicação divulgado aos seus colaboradores para reportar possíveis casos

Backup: *the HPGM group maintains a backup process to allow the recovery of its systems, such process was designed to attend to operational and legal requirements, including business continuity in case of failure, incident, or any disruptive event.*

Management: *HPGM Group monitors its environments, both physical and logical, aiming at the effectiveness of the controls in place to protect its assets, reputation, and the identification of events or alerts regarding information safety and security.*



Risk management: *The Cybersecurity area identifies and assesses the cybersecurity risks and adopts best practices for management and control.*

Change Management: *The progress and outcome of a change, mainly in the systems and infrastructure of the HPGM Group, need to follow the controls related to availability, integrity, confidentiality, and authenticity of the information and are executed only by the IT Department.*

Business Continuity: *The procedures of Business Continuity Management must be*

Incident Reporting: *HPGM Group has a clear line of communication announced to its employees to report allegations of*

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	7 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	8 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

de incidentes de segurança da informação: *information security incidents:*
cybersecurity@hedgepointglobal.com. . cybersecurity@hedgepointglobal.com.

Proteção de Dados Pessoais: A HPGM respeita a privacidade, e implementa a proteção da disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais.

Data Protection: HPGM group respects the privacy and implements the protection of availability, integrity, and confidentiality of personal data throughout its life cycle, in any form of storage or media, handling it as confidential information.



Revisão e Atualização: A HPGM possui e mantém um programa de revisão/atualização desta PSI e das Políticas Complementares sempre que se fizer necessário, visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos e atualizados.

Review and Update: HPGM Group keeps a program to review and update this ISP and the Complementary Policies whenever needed, to ensure that all security and legal technical requirements are implemented and up to date.

Dúvidas: Qualquer dúvida relativa a esta PSI deve ser encaminhada ao Departamento de Cybersecurity por meio do endereço eletrônico:
cybersecurity@hedgepointglobal.com.

Questions: Any questions regarding this ISP must be submitted to the Cybersecurity Department through the e-mail address:
cybersecurity@hedgepointglobal.com.

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	8 / 9

	Tipo de documento <i>Document Type</i>	Código Interno <i>Internal Code</i>	Páginas <i>Pages</i>
	Política Corporativa <i>Corporate Policy</i>	POL-CYB/GB-002	9 / 9
Publicidade <i>Publicity</i>	Nome do documento <i>Document Name</i>	Vigente desde <i>Effective since</i>	Versão <i>Version</i>
	Política de Segurança da Informação <i>Information Security Policy</i>	Aug/2022	01/2022

6. Legislação / Regulação Relacionada

6. Legislation / Regulation Related

Regulador	Resolução	Regulator	Resolution
CVM	Resolução 35	CVM	Resolução 35
BCB	Resolução 4893	BCB	Resolução 4893
LGPD	Lei N. 13.709/2018	LGPD	Lei N. 13.709/2018
GDPR	Regulation (EU) 2016/679	GDPR	Regulation (EU) 2016/679
CCPA	Act AB-375	CCPA	Act AB-375
NFA	9070 - NFA Compliance Rules 2-9, 2-3 and 2-49: Information Systems Security Programs	NFA	9070 - NFA Compliance Rules 2-9, 2-3 and 2-49: Information Systems Security Programs

	Tipo de documento <i>Document Type</i>	Páginas <i>Pages</i>
	Política Corporativa – Versão Pública <i>Corporate Policy – Public Version</i>	9 / 9