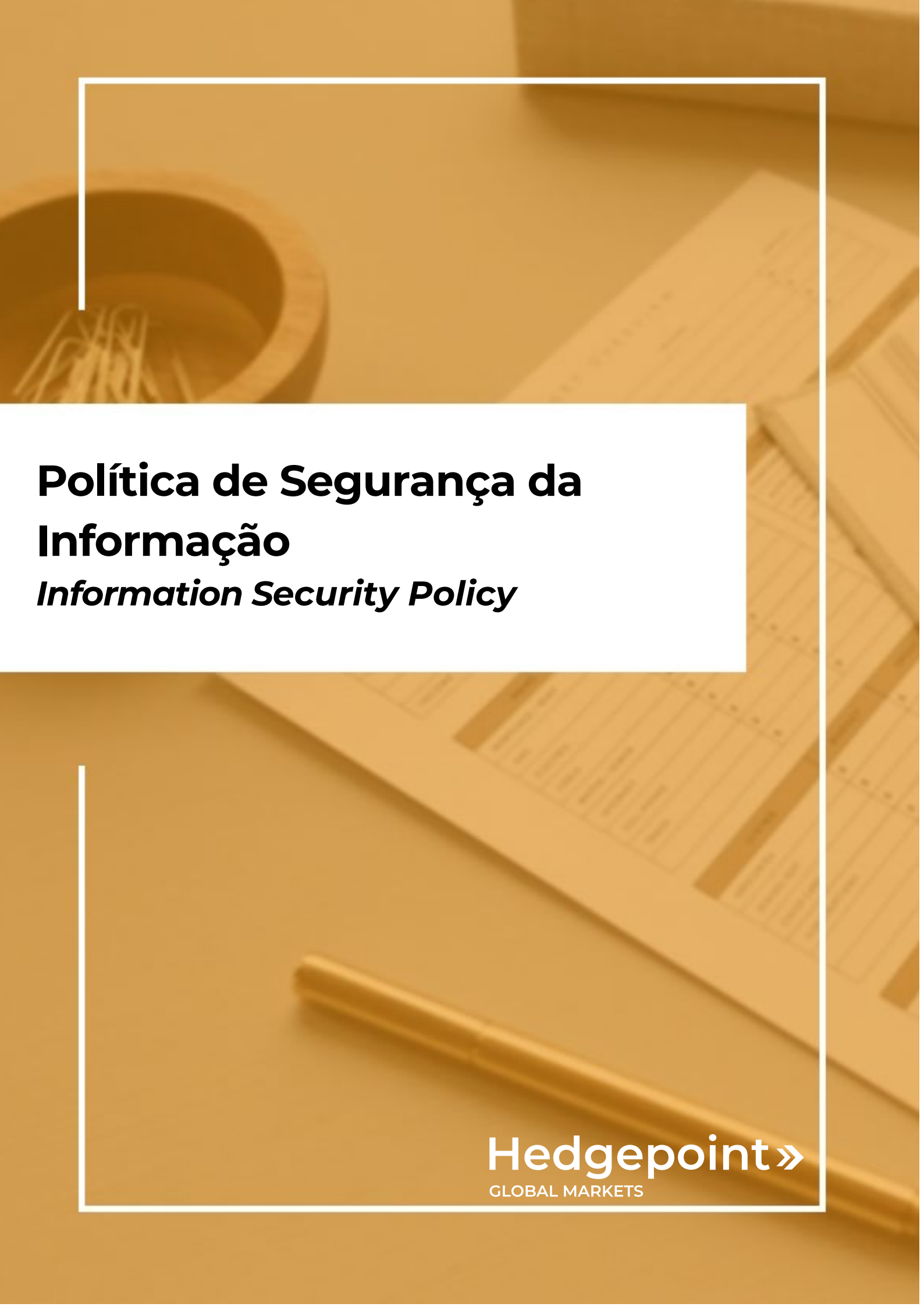

# Política de Segurança da Informação

***Information Security Policy***

Hedgepoint»
GLOBAL MARKETS

## Informações Gerais | *General Information*

| | |
|---|---|
| **Título | *Title:*** | Política de Segurança da Informação | *Information Security Policy* |
| **Referência | *Reference:*** | POL-CYB/GBL-001 |
| **Versão | *Version:*** | 4 |
| **Vigência | *Expiration date:*** | 1 ano | *year* |
| **Área Responsável | *Responsible Area:*** | Departamento de Segurança Cibernética | *Cybersecurity Department* |
| **Escopo | *Scope:*** | Global |
| **Principais Leis e Regulamentos Relacionados** ***Related Laws and Regulations*** | **Brasil | Brazil**<br>• CVM N° 35, DE 26 DE MAIO DE 2021<br>• LEI N° 13.709, DE 14 DE AGOSTO DE 2018 (LGPD)<br>• Resolução CMN n° 5.274 de 18/12/2025<br>• Resolução CMN n° 5274 e 538 de 18/12/2025<br>**EUA | US**<br>• California Consumer Privacy Act (CCPA)<br>• 9070 - NFA Compliance Rules 2-9, 2-36 and 2-49: Information System Security Programs<br>**EUROPE**<br>Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR)<br>**REFERENCE FRAMEWORKS - Brasil | Brazil**<br>• ABNT NBR ISO/IEC 27002:2022 Segurança da informação, segurança cibernética e proteção à privacidade – Controle de segurança da informação | Information security, cybersecurity and privacy protection - Information security controls.<br>• ABNT NBR ISO/IEC 27001: Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos | Information security, cybersecurity and privacy protection - Information security management systems – Requirements.<br>• ABNT NBR ISO/IEC 27701: Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e diretrizes | Security techniques - Extension to ABNT NBR /SO/IEC 27001 and ABNT NBR /SO/IEC 27002 for privacy information management-Requirements and guidelines<br>• The NIST Cybersecurity Framework (CSF) 2.0. |
| **Principais Políticas e Procedimentos Relacionadas** **Main *Related Policies and Procedures*** | • Política de Gestão de Identidades e Acessos | *Identity and Access Management Policy*<br>• Política de Classificação da Informação | *Information Classification Policy*<br>• Código de Conduta Ética e Integridade | *Code of Ethical Conduct and Integrity*<br>• Política de Treinamento e Certificações | *Training and Certification Corporate Policy*<br>• Política de Gestão de Continuidade de Negócios | *Business Continuity Management Policy* |

| | |
|---|---|
| | • Política de Desenvolvimento de Sistemas, Projetos e Inovações \| *Developing Systems, Projects and Innovations Policy*<br>• Procedimento de Avaliação de Impacto nos Negócios \| *Business Impact Analysis Procedure*<br>• Procedimento de segurança para usuários finais de arquivos críticos não-sistêmicos \| *Security proceeding for end users of non-standard critical files*<br>• Termo de Referência do Comitê de Segurança da Informação \| *Information Security Committee Term of Reference*<br>• Procedimento de Uso de Inteligência Artificial (IA) \| *Procedure for Using Artificial Intelligence*<br>• Plano de Resposta a Incidentes \| *Incident Response Plan* |
| **Audiência \| *Audience*** | Uso Restrito \| *Restricted Use* |

## Histórico de versões | *Version History*

| Versão \| *Version* | Histórico \| *Historic* | Data \| *Date* |
|---|---|---|
| 4 | Revisão e/ou atualização dos Tópicos: Siglas e Definições: Inclusão do tópico com inserção das siglas e definições do documento; Diretrizes Gerais - BYOD (Bring Your Own Device): (Inclusão de diretrizes formais sobre BYOD.); Diretrizes Gerais - Uso de Inteligência Artificial (IA): (Controles relacionados ao uso de Inteligência Artificial (IA)). Diretrizes Gerais - Plano de Resposta a Incidente: (Inclusão do acionamento do plano de resposta a incidentes); Diretrizes Gerais - Plano de Contingência: (Inclusão do acionamento em caso de incidentes de alto risco); Diretrizes Gerais - Comunicação e Escalonamento de Incidentes de Segurança: (estabelecendo a obrigatoriedade de reporte de incidentes cibernéticos e/ou vazamentos de dados à área de Compliance e, quando aplicável, aos órgãos reguladores competentes; \|<br><br>*Review and/or update of the following topics: Acronyms and Definitions: Inclusion of the topic with the insertion of the document's acronyms and definitions; General Guidelines - BYOD (Bring Your Own Device): (Inclusion of formal guidelines on BYOD); General Guidelines - Use of Artificial Intelligence (AI): (Controls related to the use of Artificial Intelligence (AI)); General Guidelines - Incident Response Plan: (Inclusion of the activation of the incident response plan); General Guidelines - Contingency Plan: (Inclusion of activation in case of high-risk incidents); General Guidelines - Communication and Escalation of Security Incidents: (establishing the mandatory reporting of cyber incidents and/or data breaches to the Compliance area and, when applicable, to the competent regulatory bodies).* | 15-06-2026<br>2025-06-15 |
| 3 | Revisão e/ou atualização dos Tópicos: Diretrizes Gerais - Ambientes Lógicos: Ambientes Lógicos (inclusão das Tecnologias utilizadas; Software Development and Acquisition (inclusão da Política de Desenvolvimento de Sistemas, Projetos e Inovações); Inclusão de atribuição do capítulo "Responsabilidades" para o Departamento de Segurança Cibernética e Diretoria de TI (inclusão da análise do SOC Report para as empresas AWS, ADP, Smarsh e Global Relay). \|<br><br>*Review and/or update of the following topics: General Guidelines - Logical Environments: Logical Environments (inclusion of the Technologies used); Software Development and Acquisition (inclusion of the Systems Development, Projects and Innovations Policy); Inclusion of the assignment of the "Responsibilities" chapter to the Cybersecurity Department and IT Directorate (inclusion of the analysis of the SOC Report for the companies AWS, ADP, Smarsh and Global Relay).* | 10-03-2025<br>2025-03-10 |
| 2 | Revisão dos Tópicos: Controle de Acesso (III e IV); Ambientes Lógicos (IV); Monitoramento; Gestão de Riscos Cibernéticos; Comitê de Segurança da Informação (CSI); Capacitação; Área de Data Privacy (DPO); Departamento Jurídico; Departamento de Recursos Humanos. \|<br><br>*Review of Topics: Access Control (III and IV); Logical Environments (IV); Monitoring; Cyber Risk Management; Information Security Committee (CSI); Training; Data Privacy Area (DPO); Legal Department; Human Resources Department.* | 14-03-2024<br>2024-03-14 |
| 1 | Criação do Documento \| *Document creation* | 30-08-2022<br>2022-08-30 |

Sumário | *Summary:*

## 1. Introdução | *Introduction*

A Hedgepoint Global Markets ("Hedgepoint" ou "Grupo Hedgepoint") 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.

Este documento dispõe sobre diretrizes e estratégias adotadas pela Hedgepoint, relacionadas às atividades de segurança cibernética, modelo de governança de Segurança da Informação e proteção de suas informações, dados e recursos de TI.

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

É responsabilidade de TODOS, independentemente de cargo ou função, estarem cientes e cumprirem a PSI da HPMG, além de aplicá-la constantemente nas suas atividades diárias, respeitando e disseminando seu conteúdo.

Hedgepoint Global Markets ("Hedgepoint" or "Hedgepoint 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 document provides guidelines and strategies to be adopted by Hedgepoint Group related to cyber-security activities, the IT governance model and the protection of information, assets, and data.

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

Regardless of job title or role, it is everyone's responsibility to be aware of and comply with Hedgepoint's ISP. All employees must apply it constantly in their day-by-day activities, observing, and conveying the content.

## 2. Objetivo | *Purpose*

A PSI é o documento que expressa o posicionamento do Grupo Hedgepoint 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 Hedgepoint, na promoção de diretrizes estratégicas, responsabilidades, competências, apoio e melhoria contínua 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 Hedgepoint em relação à Segurança da Informação, reforçando a cultura interna e priorizando as ações necessárias conforme negócio;

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

The ISP expresses the position of Hedgepoint 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 Hedgepoint Group to the promotion of the strategic framework, responsibilities, skills, and continuous support and improvement to the Information Security Management System (ISMS) in order to ensure the protection of its tangible and intangible assets.

II. To establish responsibilities and boundaries of the Hedgepoint Group employees concerning Information Security, reinforcing an internal culture and prioritizing the necessary actions according to the business.

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

## 3. Princípios | *Principles*

| | |
|---|---|
| Preservar e proteger as informações do Grupo Hedgepoint ou sob sua reponsabilidade de vulnerabilidades e ameaças, em todo o seu ciclo de vida, contida em qualquer suporte ou formato.<br><br>Prevenir e reduzir impactos gerados pelos incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades profissionais.<br><br>No âmbito de suas obrigações e responsabilidades, zelar por relações transparentes e éticas nos termos do Código de Conduta Ética e Integridade.<br><br>Cumprir as legislações relacionadas ao negócio no que diz respeito à segurança da informação, assim como as legislações vigentes em cada país de atuação. | Preserve and protect the information of the Hedgepoint Group, or under its responsibility, from vulnerabilities and threats throughout its lifecycle, contained in any media or format.<br><br>Prevent and reduce the impacts of information security incidents, ensuring confidentiality, integrity, availability, authenticity, and legitimacy in the development of professional activities.<br><br>Within the scope of their obligations and responsibilities, ensure transparent and ethical relationships in accordance with the Code of Ethical Conduct and Integrity.<br><br>Comply with the industry related legislation regarding IS, including the laws in force in each country Hedgepoint operates. |

## *4.* Escopo | Scope

| | |
|---|---|
| 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 Hedgepoint 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 Hedgepoint Group including its computer network. |

## 5. Responsabilidades pela Execução desta Política | Roles accountable for executing this policy

| | |
|---|---|
| **Diretoria de TI**<br><br>O CTO é responsável por:<br><br>I. Analisar, aprovar e declarar formalmente o seu comprometimento com esta PSI.<br><br>II. Aprovar os investimentos em SI na Hedgepoint, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio.<br><br>III. Analisar e aprovar, ou não, as exceções de forma excepcional a essa PSI. | ***Director of IT***<br><br>The CTO is responsible for:<br><br>I. Analyze, approve, and declare the commitment with this PSI formally.<br><br>II. Approve the investment in Information Security at Hedgepoint Group, considering the feasibility and its impact on the quality of business processes.<br><br>III. Review and approve, or deny, the exceptions concerning this ISP. |
| **Comitê de Tecnologia, Privacidade e Segurança da Informação** | **Technology, Privacy and Information Security Committee** |

| | |
|---|---|
| I. As atribuições do Comitê de Segurança da Informação (CSI) estão descritas no Termo de Referência do Comitê de Segurança da Informação. | I. The responsibilities of the Information Security Committee (ISC) are described in the Cybersecurity Committee Term of Reference. |
| **Departamento de Segurança Cibernética**<br><br>I. Promover e realizar a gestão do SGSI, garantindo a implementação de controles, modelos, padrões e recursos necessários para a proteção da informação.<br><br>II. Promover a cultura de SI no Grupo Hedgepoint;<br><br>III. Analisar e priorizar ações necessárias, balanceando custo e benefício.<br><br>IV. Auxiliar, sempre que necessário, na capacitação dos colaboradores em SI.<br><br>V. Aprovar os investimentos em SI no Grupo Hedgepoint, juntamente com a CTO, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio.<br><br>VI. Revisar os relatórios anuais SOC (System and Organization Controls) dos principais fornecedores de tecnologia que emitem esse tipo de relatório (como Smarsh, Global Relay Communications Inc., AWS e Microsoft), bem como, quando necessário, de outros fornecedores críticos. Além disso, analisar os incidentes de Segurança da Informação reportados e, sempre que aplicável, submeter relatório para deliberação do CTO.<br><br>VII. Identificar e avaliar os riscos relacionados à segurança da informação e propor melhorias e recursos necessários às ações de segurança da informação.<br><br>VIII. Realizar e acompanhar estudos de tecnologias, com o apoio da área de Infraestrutura, quanto a possíveis impactos na segurança da informação e/ou na Infraestrutura.<br><br>IX. Manter atualizado os documentos que compõem o SGSI.<br><br>X. Propor, processos e procedimentos internos relativos à segurança da informação no Grupo Hedgepoint.<br><br>XI. Monitorar os acessos aos ambientes lógicos do Grupo Hedgepoint.<br><br>XII. Avaliar se os requisitos de segurança da informação estão presentes antes da aquisição, manutenção ou desenvolvimento de softwares. | **Cybersecurity Departament**<br><br>I. Promote and carry out the management of the ISMS and ensure the implementation of the controls, templates, patterns, and resources that are necessary for the protection of the information.<br><br>II. Promote an Information Security culture in the Hedgepoint Group.<br><br>III. Analyze and prioritize the actions needed, balancing the cost and benefits.<br><br>IV. Assist, whenever it is necessary, in the IS training process of Hedgepoint's employees.<br><br>V. Approve the investment in Cybersecurity at Hedgepoint Group, in conjunction with the Head of IT, considering the feasibility and its impact on the quality of the business processes.<br><br>VI. Review the annual SOC (System and Organization Controls) reports from key technology vendors that issue this type of report (such as Smarsh, Global Relay Communications Inc., AWS, and Microsoft), as well as, when necessary, from other critical vendors. Additionally, analyze reported Information Security incidents and, whenever applicable, submit a report for CTO deliberation.<br><br>VII. Identify and assess the risks related to information security and propose improvements and resources that are necessary to mitigate risks.<br><br>VIII. To conduct and monitor technology studies, with the support of the Infrastructure area, regarding potential impacts on information security and/or infrastructure.<br><br>IX. Keep updated all the documents that are part of the ISMS.<br><br>X. Propose processes and procedures related to information security in the Hedgepoint Group.<br><br>XI. Monitor access to the logical environments.<br><br>XII. Evaluate the information security requirements that are present before the acquisition, maintenance, or software development.<br><br>XIII. Ensure that the progress and the outcome of changes do not negatively impact the existing controls related to availability, integrity, |

| | |
|---|---|
| XIII. Garantir o andamento e o resultado de mudanças preservem os controles relacionados à disponibilidade, integridade, confidencialidade, autenticidade e legalidade das informações, sobretudo nos sistemas e na infraestrutura tecnológica.<br><br>XIV. Solicitar, quando couber, procedimento disciplinar para apuração de responsabilidades dos envolvidos em violações de segurança da informação, deliberar a violação com os Departamentos de RH, Compliance e Jurídico e notificar os devidos responsáveis para aplicar as penalidades, quando necessário. | confidentiality, authenticity, and legitimacy of that information, particularly on systems and Infrastructure.<br><br>XIV. When applicable, request disciplinary proceedings to determine the responsibilities of those involved in information security violations, deliberate the matter with the HR, Compliance, and Legal Departments, and notify the appropriate parties to apply penalties, when necessary. |
| **Encarregado pelo Tratamento de Dados Pessoais (DPO)**<br><br>I. Assegurar que as medidas de segurança e organizacionais de proteção de dados estejam em vigor.<br><br>II. Assegurar que os funcionários do Grupo Hedgepoint estejam cientes das políticas e práticas de privacidade de dados e recebam treinamento adequado sobre elas.<br><br>III. Monitorar a conformidade com leis e regulamentações de privacidade e proteção de dados (como o GDPR, LGPD, CDPA e CCPA) com o apoio das áreas de Compliance e Jurídico e garantir que os processos internos estejam alinhados.<br><br>IV. Estabelecer processos para atender aos pedidos dos indivíduos relacionados a seus direitos, como acesso, retificação, exclusão, oposição, portabilidade, entre outros.<br><br>V. Fornecer orientação sobre avaliações de impacto, implementação de medidas de privacidade por design e padrão, e outras considerações relacionadas à privacidade. | ***Data Privacy Officer (DPO)***<br><br>I. Ensure that data protection security and organizational measures are in place.<br><br>II. Ensure that Hedgepoint Group employees are aware of data privacy policies and practices and receive appropriate training on them.<br><br>III. Monitor compliance with privacy and data protection laws and regulations (such as GDPR, LGPD, CDPA, and CCPA) with the support of the Compliance and Legal departments and ensure that internal processes are aligned.<br><br>IV. Establish processes to address individual requests related to their rights, such as access, rectification, deletion, objection, portability, among others.<br><br>V. Provide guidance on impact assessments, implementation of privacy by design and standard measures, and other privacy-related considerations. |
| **Departamento Jurídico**<br><br>I. Participar, apoiar e orientar, de acordo com os aspectos jurídicos, os processos de contratação e as exigências legislativas relacionadas à segurança da informação;<br><br>II. Redigir, revisar e atualizar os contratos com terceiros (como fornecedores e parceiros), para assegurar que as cláusulas de segurança da informação sejam abrangentes e vinculativas.<br><br>III. Aconselhar sobre as implicações legais de qualquer incidente de segurança da informação e orientar a | ***Legal Department***<br><br>I. Participate, support, and guide, in accordance with legal aspects, the contracting processes and legislative requirements related to information security.<br><br>II. Draft, review, and update contracts with third parties (such as suppliers and partners) to ensure that information security clauses are comprehensive and binding.<br><br>III. Advise on the legal implications of any information security incident and guide the organization |

| | |
|---|---|
| organização durante o processo de notificação a reguladores e partes afetadas.<br>IV. Representar o Grupo Hedgepoint em quaisquer litígios ou disputas que possam surgir devido a incidentes de segurança ou violações de contrato relacionadas à segurança da informação.<br>V. Fornecer aconselhamento proativo as áreas do Grupo Hedgepoint sobre riscos legais relacionados à segurança da informação. | through the notification process to regulators and affected parties.<br>IV. Represent the Hedgepoint Group in any litigation or disputes that may arise due to security incidents or contract breaches related to information security.<br>V. Provide proactive advice to the areas of the Hedgepoint Group on legal risks related to information security. |
| **Departamento de Recursos Humanos**<br>I. Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores.<br>II. Comunicar ao time de Segurança Cibernética qualquer admissão e/ou demissão de colaboradores, assim como mudança entre departamentos do Grupo Hedgepoint.<br>III. Lidar com quaisquer incidentes de segurança que envolvam funcionários, como vazamentos de dados intencionais, e trabalhar em conjunto com a área de Segurança Cibernética, Compliance e Jurídico para investigar e resolver tais incidentes.<br>IV. Custodiar e colher assinatura do "Termo de Ciência e Responsabilidade" na admissão de novos colaboradores.<br>V. Assegurar e controlar que todos os colaboradores recebam treinamentos adequados e atualizados para manter a segurança da informação. | ***Human Resource Department***<br>I. Provide security controls specifically related to the processes of hiring, termination, and modification of the activities of the employees.<br>II. Notify the Cybersecurity team of any hiring and/or termination of employees, as well as transfers between departments within the Hedgepoint Group.<br>III. Handle any security incidents involving employees, such as intentional data leaks, and collaborate with the Cybersecurity, Compliance, and Legal departments to investigate and resolve such incidents.<br>IV. Ensure and obtain signatures on the 'Acknowledgment and Responsibility Agreement' upon the admission of new employees.<br>V. Ensure that all employees receive adequate and up-to-date training to maintain information security. |
| **Departamento de Compliance**<br>I. Garantir a publicidade e disponibilidade das Políticas e Procedimentos (P&Ps) que compõe o SGSI do Grupo Hedgepoint que é coordenado por Comunicação Interna. | ***Compliance Department***<br>I. Ensure the publicity and availability of the Policies & Procedures that comprise the Information Security Management System of Grupo Hedgepoint, which is coordinated by Internal Communications. |
| **Departamento de Comunicação e Marketing**<br>I. Autorizar ou não, o uso das marcas, identidade visual e qualquer outro sinal distintivo atual ou futuro do Grupo Hedgepoint – nos usos internos e externos, visando garantir uso adequado do padrão vigente no Brand System, bem como autorização formal por uso da marca por algum fornecedor, seja para padronizar ferramentas, ou outros usos como nos referir como caso de sucesso ou referência, por exemplo. | ***Communication and Marketing Department***<br>I. Authorize or deny the usage of trademarks, visual identity, and any other current or future distinctive sign of the Hedgepoint Group - in internal and external uses, to ensure adequate use of current standards in the Brand System, as well as formally authorize the usage of the brand by a supplier, whether to standardize a tool or for other cases, such as commercial references. |

| | |
|---|---|
| II. Dar suporte através de campanhas e divulgação relacionados ao tema segurança da informação – por meio do time de comunicação interna. | II. Carry out campaigns and dissemination of Information Security, through the internal communication team. |
| **Gestor da Informação**<br><br>I. Autorizar, de forma criteriosa, a revelação de qualquer informação de propriedade ou sob a responsabilidade do Grupo Hedgepoint.<br><br>II. Identificar violações ou qualquer ação duvidosa praticada pelos colaboradores no uso da informação do Grupo Hedgepoint e comunicar ao time de Segurança Cibernética e ao time do Compliance. | ***Information Owner***<br><br>I. Authorize or deny, the disclosure of any information owned or under the responsibility of the Hedgepoint Group.<br><br>II. Identify violations or any questionable actions related to the usage of Hedgepoint Group's information, such facts should be communicated to the Cybersecurity team and Compliance team. |
| **Gestores, Coordenadores e Líderes**<br><br>I. Garantir e gerenciar o cumprimento desta PSI e demais documentos complementares pelos seus colaboradores;<br><br>II. Identificar as possíveis vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio.<br><br>III. Autorizar, ou não, a utilização de Recursos de TI ou dispositivos móveis particulares por seus colaboradores para execução de qualquer atividade profissional no Grupo Hedgepoint.<br><br>IV. Garantir que os ativos de propriedade ou sob a responsabilidade, sejam utilizados com cuidado e de acordo com as orientações do fabricante e da empresa;<br><br>V. Aplicar, após definição com o Departamento de Recursos Humanos, Compliance e Jurídico, as sanções de violação desta PSI e documentos complementares;<br><br>VI. Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por seus colaboradores, comunicando o cybersecurity@hedgepointglobal.com imediatamente. | **Managers, Coordinators and Leaders**<br><br>I. Ensure and manage compliance with this ISP and with other complementary documents by their employees.<br><br>II. Identify and assess potential vulnerabilities and threats in the processes and activities for which they are responsible, which must be dealt with diligence to reduce impacts on the business.<br><br>III. Authorize, or deny, the usage of IT resources or private mobile devices by their employees for the execution of any professional activity in the Hedgepoint Group.<br><br>IV. Ensure that assets owned or under Hedgepoint's responsibility are used with care and following manufacturer and company guidelines.<br><br>V. Apply, after agreement with Human Resources and Legal Departments, the sanctions for the violation of this PSI or complementary documents.<br><br>VI. Identify information security incidents or any suspect action carried out by their employees, by communicating cybersecurity@hedgepointglobal.com immediately. |
| **Colaboradores, Estagiários**<br><br>I. Estar ciente e manter-se atualizado com esta PSI e demais documentos complementares;<br><br>II. Conhecer e assinar o "Termo de Ciência e Responsabilidade";<br><br>III. Utilizar os ativos de propriedade do Grupo Hedgepoint ou sob sua responsabilidade de acordo | ***Employees, Interns***<br><br>I. Be aware of and keep up to date with this ISP and other supplementary documents.<br><br>II. Read and sign the "Term of Responsibility".<br><br>III. Use the assets owned by the Hedgepoint Group or under its responsibility following the guidelines of |

| | |
|---|---|
| com as orientações do fabricante, do desenvolvedor e da empresa, com cuidado e zelo; | the manufacturer, developer, and the company with care. |
| IV. Utilizar os ativos e informações do Grupo Hedgepoint somente para fins profissionais, de forma ética e legal, respeitando os direitos e as permissões de uso concedidas; | IV. Use the assets and information of Hedgepoint Group for professional purposes only, ethically, and legally, respecting the rights and permissions of the granted usage. |
| V. Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na Internet; | V. Preserve the integrity, availability, confidentiality, authenticity, and legality of the information accessed or manipulated by not using, sending, transmitting, or sharing it improperly in any location or media, including on the Internet. |
| VI. Não revelar qualquer informação de propriedade ou sob a responsabilidade do Grupo Hedgepoint sem a prévia e formal autorização; | VI. Do not disclose any information owned or under the responsibility of the Hedgepoint Group without prior and formal authorization. |
| VII. Utilizar as marcas e outros sinais distintivos, patentes, desenhos industriais, softwares e demais direitos de propriedade intelectual de titularidade do Grupo Hedgepoint somente para finalidades profissionais e autorizadas pela empresa, de acordo com a atividade e função exercida; | VII. Use the trademarks and other distinctive signs, patents, industrial designs, software, and other intellectual property rights owned by the Hedgepoint Group for professional purposes and only when previously authorized by the company, according to the activity and function performed. |
| VIII. Zelar pela segurança da sua identidade digital, não compartilhando, divulgando ou transferindo a terceiros; | VIII. Ensure the security of your digital identity by not sharing, disclosing, or transferring to third parties. |
| IX. Responder por toda e qualquer atividade realizada nos Recursos de TI, mediante o uso de sua identidade digital; | IX. Be responsible for any activity carried out on the IT resources, through the usage of your digital identity. |
| X. Cumprir as legislações listadas no Capítulo de Informações Gerais deste documento e demais instrumentos regulamentares relacionados às atividades profissionais; | X. Comply with legislations listed in Chapter General Information of this document and other regulatory instruments related to professional activities. |
| XI. Reportar formalmente ao seu Gestor quaisquer eventos relativos à violação ou possibilidade de violação de segurança ou atividades suspeitas. | *XI.* Formally report to your manager any event related to the security breach or possibility of a security breach or any suspicious activity |

## 6. Siglas e Definições | Acronyms and Definitions

| | |
|---|---|
| **Acesso Físico**: Tipo de acesso presencial a um local / ambiente que pode ser restrito ou permitido, dependendo das políticas e medidas de segurança implementadas no local. | **Physical Access:** Type of in-person access to a location/environment that may be restricted or permitted, depending on the security policies and measures implemented on-site. |
| **Acesso Lógico**: Tipo de acesso que controle as autorizações de acesso virtual aos recursos tecnológicos da empresa, dadas aos seus colaboradores, de forma a preservar os aspectos de | **Logical Access**: Type of access that controls virtual access authorizations to the company's technological resources, given to its employees, in order to preserve Information Security aspects throughout its lifecycle within the company. |

| | |
|---|---|
| Segurança das Informações durante todo o seu ciclo de vida na empresa.<br><br>**Ambientes Físicos**: Todos os ambientes e áreas, sob o ponto de vista de acesso físico, do Grupo.<br><br>**Apetite de Riscos:** É o nível de incerteza e exposição a perdas que a empresa está disposta a aceitar na busca por objetivos estratégicos e recompensas. Definido pela alta gestão, ele orienta decisões de negócios, equilibrando segurança e crescimento, e diferencia riscos aceitos (baixo, médio) de riscos que exigem tratamento imediato (alto).<br><br>**Aplicativos**: É um software projetado para executar tarefas específicas de interesse da empresa visando facilitar a vida dos usuários, atuando desde funções simples como calcular e pesquisar até tarefas complexas, como suporte a programas e sistemas.<br><br>**Ativos de Informação**: Conjunto de todos os recursos tecnológicos da empresa usados no tratamento de informações de propriedade e/ou sob custódia da empresa.<br><br>**Autenticação**: A Autenticação é a capacidade de um sistema ou aplicativo confirmar positiva ou negativamente uma determinada identidade de acesso.<br><br>**Autenticidade da Informação**: Característica que garante que uma informação seja autêntica, verdadeira e incontestável em sua origem e conteúdo porque foi obtida e tratada pelos meios adequados de segurança e conformidade legal.<br><br>**Backup:** É o ato de fazer cópias de segurança de um ambiente, aplicação ou dados em um determinado momento.<br><br>**BYOD (Bring Your Own Device):** É uma diretriz de TI que estabelece regras onde colaboradores utilizam seus aparelhos pessoais como smartphones, notebooks e tablets para atividades de trabalho e acesso a dados corporativos.<br><br>**CAB (Change Adivisory Board):** Conselho Consultivo de Mudanças, é um grupo de especialistas (TI e negócios) responsável por avaliar, priorizar e aprovar/rejeitar mudanças significativas na infraestrutura ou serviços de TI.<br><br>**Cibersegurança / Segurança Cibernética**: Ramo da segurança que atua nos aspectos de segurança tecnológica para controlar acessos, identidades e permissões dos usuários dentro do Grupo. | **Physical Environments**: All environments and areas, from the point of view of physical access, of the Group.<br><br>**Risk Appetite**: It is the level of uncertainty and exposure to losses that the company is willing to accept in the pursuit of strategic objectives and rewards. Defined by senior management, it guides business decisions, balancing security and growth, and differentiates acceptable risks (low, medium) from risks that require immediate treatment (high).<br><br>**Applications**: This is software designed to perform specific tasks of interest to the company, aiming to make users' lives easier, ranging from simple functions such as calculating and searching to complex tasks such as program and system support.<br><br>**Information Assets**: The set of all technological resources of the company used in the processing of information owned and/or under the custody of the company.<br><br>**Authentication**: Authentication is the ability of a system or application to positively or negatively confirm a given access identity.<br><br>**Information Authenticity**: A characteristic that guarantees that information is authentic, true, and indisputable in its origin and content Security and legal compliance.<br><br>**Backup**: This is the act of making security copies of an environment, application, or data at a given time.<br><br>**BYOD (Bring Your Own Device)**: This is an IT guideline that establishes rules where employees use their personal devices such as smartphones, laptops, and tablets for work activities and access to corporate data.<br><br>**CAB (Change Advisory Board)**: The Change Advisory Board is a group of experts (IT and business) responsible for evaluating, prioritizing, and approving/rejecting significant changes to IT infrastructure or services.<br><br>**Cybersecurity**: The branch of security that deals with technological security aspects to control access, identities, and user permissions within the Group.<br><br>**Cryptography**: The process of converting readable information (plaintext) into a scrambled and |

| | |
|---|---|
| **Criptografia:** Processo de converter informações legíveis (texto claro) em um formato embaralhado e ilegível (texto cifrado) para proteger a confidencialidade dos dados. | unreadable format (ciphertext) to protect data confidentiality. |
| **Cofre de Senhas:** Gerenciador de senha ou armário de senha, é um espaço criptografado usado para armazenar dados, como senhas e credenciais de login (as informações usadas para acessar aplicativos e contas digitais), documentos, imagens e outras informações confidenciais em um local digital. | **Password Vault**: A password manager or password cabinet is an encrypted space used to store data such as passwords and login credentials (the information used to access applications and digital accounts), documents, images, and other confidential information in a digital location. |
| **Colaboradores**: Todos os tipos de empregados, funcionários, prestadores de serviços, estagiários, gestores, administradores, diretores ou afins que atuam na empresa profissionalmente, independentemente de ter ou não vínculo empregatício. | **Collaborators**: All types of employees, staff, service providers, interns, managers, administrators, directors, or similar individuals who work professionally at the company, regardless of whether or not they have an employment relationship. |
| **EUC - End-User Computing (Computação de Usuário Final):** Conjunto de tecnologias, políticas e ferramentas que permite aos funcionários acessarem com segurança, de qualquer lugar e dispositivo, os dados, aplicativos e áreas de trabalho (desktops) de que precisam para trabalhar. | **EUC - End-User Computing**: A set of technologies, policies, and tools that allows employees to securely access, from anywhere and any device, the data, applications, and desktops that they need to work. |
| **Comitê de Segurança da Informação (CSI):** Órgão deliberativo e estratégico, formado por líderes e gestores, com a finalidade de estabelecer diretrizes, normas e políticas para proteger os dados (confidencialidade, integridade, disponibilidade) e garantir a conformidade legal (como a LGPD) de uma organização. | **Information Security Committee (CSI)**: A deliberative and strategic body, formed by leaders and managers, with the purpose of establishing guidelines, standards and policies to protect data (confidentiality, integrity, availability) and ensure legal compliance (such as the LGPD) of an organization. |
| **Comitê de Tecnologia, Privacidade e Segurança da Informação (CTPSI):** Responsável por definir e manter a estrutura de controles de privacidade e segurança da informação, bem como, promover as boas práticas por meio de disponibilização de guias, processos, modelos e procedimentos relacionados à temática. | **Technology, Privacy and Information Security Committee (CTPSI)**: Responsible for defining and maintaining the structure of privacy and information security controls, as well as promoting best practices by means of providing guides, processes, models, and procedures related to the topic. |
| **Confidencialidade das Informações**: Característica de segurança que garante o sigilo dos dados, assegurando que apenas pessoas ou sistemas autorizados possam acessá-los e manipulá-los. | **Confidentiality of Information**: Security feature that guarantees the confidentiality of data, ensuring that only authorized people or systems can access and manipulate it. |
| **Need to know (Conhecimento Estritamente Necessário)**: Princípio da Necessidade de saber que é um conceito de segurança da informação que determina que um usuário deve ter acesso somente aquilo que realmente necessita saber para executar as suas funções, limitando assim o potencial de dano em caso de comprometimento ou erro e protegendo a privacidade e sigilo das informações. | **Need to know (Strictly Necessary Knowledge)**: The Need to Know principle is an information security concept that determines that a user should only have access to what they really need to know to perform their functions, thus limiting the potential for damage in case of compromise or error and protecting the privacy and confidentiality of information. |
| | **Business Continuity**: Strategic and tactical capacity of a department to plan for and respond to incidents and business interruptions, minimizing their impacts and recovering losses of information assets from critical |

| | |
|---|---|
| **Continuidade do Negócio:** Capacidade estratégica e tática de um departamento de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. | activities, in order to maintain its operations at an acceptable, previously defined level. |
| **Data Loss Prevention (DLP):** Prevenção contra Perda de Dados, é um conjunto de tecnologias, estratégias e políticas de segurança projetadas para detectar e evitar o vazamento, uso indevido ou acesso não autorizado a dados confidenciais. | **Data Loss Prevention (DLP)**: Data Loss Prevention is a set of technologies, strategies, and security policies designed to detect and prevent the leakage, misuse, or unauthorized access to confidential data. |
| **DDoS (Distributed Denial of Service):** Negação de Serviço Distribuída é uma tentativa maliciosa de tirar um site, servidor ou rede do ar, sobrecarregando-o com tráfego massivo vindo de múltiplas fontes simultâneas. | **DDoS (Distributed Denial of Service)**: Distributed Denial of Service is a malicious attempt to take a website, server, or network offline by overwhelming it with massive traffic from multiple simultaneous sources. |
| **Disponibilidade das Informações**: Característica que garante que sistemas, dados e serviços estejam acessíveis e operacionais a quem deles necessitam e tenham autorização para acessá-los, sempre que necessários, assegurando a continuidade das operações. | **Information Availability**: A characteristic that ensures that systems, data, and services are accessible and operational to those who need them and are authorized to access them, whenever necessary, ensuring business continuity. |
| **EDR (Endpoint Detection and Response):** Software de detecção e resposta de endpoint é usado pelas equipes de operações de segurança para detectar, conter, investigar e corrigir ataques. | **EDR (Endpoint Detection and Response)**: Endpoint detection and response software is used by security operations teams to detect, contain, investigate, and remediate attacks. |
| **Endpoints:** Qualquer dispositivo físico, como notebooks, smartphones, servidores ou dispositivos IoT, que se conecta e troca dados em uma rede. | **Endpoints**: Any physical device, such as laptops, smartphones, servers, or IoT devices, that connects to and exchanges data on a network. |
| **Equipamentos / Recursos Tecnológicos**: Conjunto de todos os equipamentos, hardwares, softwares e afins que a empresa coloca à disposição dos usuários para que possam conduzir suas atividades profissionais. | **Technological Equipment/Resources**: The set of all equipment, hardware, software, and the like that the company makes available to users so that they can conduct their professional activities. |
| **GDPR (General Data Protection Regulation):** Regulamento Geral sobre a Proteção de Dados da União Europeia (UE), vigente desde maio de 2018. É uma lei abrangente que regula como empresas coletam, processam e armazenam dados pessoais de residentes da UE, focando na transparência, privacidade e controle do usuário. | **GDPR (General Data Protection Regulation)**: General Regulation on Data Protection of the European Union (EU), in force since May 2018. It is a comprehensive law that regulates how companies collect, process and store personal data of UE residents, focusing on transparency, privacy, and user control. |
| **Gestão de Identidades**: Conjunto de políticas, processos e tecnologias que verifica e controla quem pode acessar a quais dados e recursos dentro da organização. O objetivo principal é garantir que apenas usuários e sistemas autorizados tenham acesso apropriado aos recursos certos, no momento | **Identity Management**: A set of policies, processes, and technologies that verify and controls who can access which data and resources within the organization. The main objective is to ensure that only authorized users and systems have appropriate access to the right resources at the right time, using mechanisms such as authentication and authorization.<br><br>**Access Management/Control**: An information security process that controls, authenticates, authorizes, and audits access to systems, data, and resources, ensuring that only authorized users can |

| | |
|---|---|
| certo, usando mecanismos como a autenticação e a autorização | interact with previously authorized information and systems. |
| **Gestão / Controle de Acessos**: Processo de segurança da informação que controla, autêntica, autoriza e audita o acesso a sistemas, dados e recursos, garantindo que apenas utilizadores autorizados possam interagir com informações e sistemas previamente autorizados. | **Information Security Incidents**: Any event that affects Confidentiality, Integrity, or Availability of data and/or information systems, resulting in operational problems, damage, or loss of information, etc. |
| **Incidentes de Segurança da Informação**: Qualquer evento que afete a Confidencialidade, Integridade ou Disponibilidade de dados e/ou sistemas de informação, resultando em problemas operacionais, dano ou perda das informações etc. | **Information Integrity**: A characteristic that ensures that data and information remain accurate, consistent, and unaltered throughout their entire lifecycle, protected against accidental or malicious alterations. |
| **Integridade das Informações**: Característica que garante que dados e informações permaneçam precisos, consistentes e inalterados ao longo de todo o seu ciclo de vida, protegidos contra alterações acidentais ou maliciosas. | **Artificial Intelligence (AI)**: The ability of machines and computer systems to simulate human cognitive functions, such as learning, reasoning, problem-solving, perception, and creativity. It processes large volumes of data, identifies patterns, and makes autonomous decisions to achieve specific objectives, continuously improving itself. |
| **Inteligência Artificial (IA)**: Capacidade de máquinas e sistemas computacionais simularem funções cognitivas humanas, como aprendizado, raciocínio, resolução de problemas, percepção e criatividade. Ela processa grandes volumes de dados, identifica padrões e toma decisões autônomas para atingir objetivos específicos, aprimorando-se continuamente. | **Legality of Information**: This means that all management and handling of information must comply with current laws and regulations, both in the creation and in the disclosure and access to data. |
| **Legalidade da Informação**: Significa que toda a gestão e manuseamento da informação devem estar em conformidade com as leis e regulamentos vigentes, tanto na criação quanto na divulgação e acesso aos dados. | **LGPD**: The LGPD is the Brazilian legislation that regulates the processing of personal data by individuals or legal entities, public or private, with the objective of protecting the fundamental rights of freedom, privacy, and the free development of the personality of the natural person. It covers physical and digital data, guaranteeing citizens control over their information. |
| **LGPD:** A LGPD é a legislação brasileira que regulamenta o tratamento de dados pessoais por pessoas físicas ou jurídicas, públicas ou privadas, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ela abrange dados físicos e digitais, garantindo ao cidadão controle sobre suas informações. | **Logs**: Logs are automatic and chronological records of events, activities, and messages generated by computer systems, applications, or networks. |
| **Logs**: Logs são registros automáticos e cronológicos de eventos, atividades e mensagens gerados por sistemas computacionais, aplicações ou redes. | **Least Privilege**: The Principle of Least Privilege is an information security concept that dictates that any user, program, or system should have only the minimum and necessary permissions to perform its functions, limiting thus, the potential for damage in case of compromise or error. |
| **Menor Privilégio (Least Privilege)**: Princípio do Menor Privilégio é um conceito de segurança da informação que determina que qualquer usuário, programa ou sistema deve ter apenas as permissões mínimas e necessárias para executar as suas funções, limitando | **Multi-Factor Authentication**: Multi-factor authentication (MFA) is a security method that requires several distinct forms of identification for a user to access a system or application, adding an extra layer of protection beyond the traditional password. The goal is to verify a user's identity through multiple |

| | |
|---|---|
| assim o potencial de dano em caso de comprometimento ou erro.<br><br>**Múltiplo Fator de Autenticação**: A autenticação de múltiplo fator (MFA) é um método de segurança que requer várias formas distintas de identificação para um usuário acessar a um sistema ou aplicação, acrescentando uma camada extra de proteção além da tradicional senha. O objetivo é verificar a identidade de um usuário através de múltiplos fatores diferentes, tornando o acesso mais seguro contra roubo de credenciais e acesso não autorizado.<br><br>**Prestadores de Serviços**: Um tipo de colaborador que executa serviços na empresa sob forma de contrato pessoal ou através da contratação com uma empresa terceirizada que o contrata e o designa para trabalhar no Grupo.<br><br>**Privileged Access Management (PAM) / Acesso Privilegiado:** São permissões concedidas a um usuário ou sistema para executar uma ou mais ações específicas ou acessar a um recurso. Já o acesso privilegiado se refere à posse e ao uso de contas com direitos administrativos ou de acesso a informações e sistemas críticos ou afins.<br><br>**Proteção de Dados na Nuvem (CASB):** Cloud Access Security Broker - Agente de Segurança de Acesso à Nuvem é uma ferramenta de software ou hardware que atua como intermediário entre usuários e provedores de nuvem, aplicando políticas de segurança, visibilidade e conformidade<br><br>**Política de Segurança da Informação (PSI):** Documento formal que estabelece diretrizes, regras e procedimentos de segurança para proteger os ativos de dados de uma organização contra ameaças internas e externas<br><br>**Recursos de TI:** Englobam todos os componentes físicos (hardware), digitais (software), redes, dados e serviços necessários para processar, armazenar e transmitir informações em uma organização.<br><br>**Repositórios Digitais:** Ferramenta tecnológica de gestão da informação e do conhecimento, formado por coleções digitais que contribuem para o armazenamento, organização, disponibilização, transparência, busca, recuperação, acesso.<br><br>**Riscos Cibernéticos:** Possibilidade de perdas financeiras, operacionais ou de reputação causadas por falhas em sistemas digitais, ataques de hackers ou vazamento de dados. | different factors, making access more secure against credential theft and unauthorized access.<br><br>**Service Providers**: A type of employee who performs services in the company under a personal contract or through contracting with a third-party company that hires and assigns them to work in the Group.<br><br>**Privileged Access Management (PAM)**: Permissions granted to a user or system to perform one or more specific actions or access a resource. Privileged access refers to the possession and use of accounts with administrative rights or access to critical or related information and systems.<br><br>**Cloud Data Protection Broker (CASB)**: Cloud Access Security Broker is a software or hardware tool that acts as an intermediary between users and cloud providers, enforcing security, visibility, and compliance policies.<br><br>I**nformation Security Policy (ISP)**: A formal document that establishes guidelines, rules, and security procedures to protect an organization's data assets against internal and external threats.<br><br>**IT Resources**: Encompass all physical (hardware), digital (software), network, data, and service components necessary to process, store, and transmit information within an organization.<br><br>**Digital Repositories**: A technological tool for information and knowledge management, consisting of digital collections that contribute to storage, organization, availability, transparency, search, retrieval, and access.<br><br>**Cyber Risks**: The possibility of financial, operational, or reputational losses caused by failures in digital systems, hacker attacks, or data leaks.<br><br>**Security by Design**: A proactive approach that integrates security measures from the initial design and architecture phase of systems, software, or infrastructure, rather than treating it as an afterthought.<br><br>**Segregation of Duties (SoD**): or Segregation of Duties is an internal control that divides critical responsibilities and tasks among different people to |

**Security by Design:** Abordagem proativa que integra medidas de segurança desde a fase inicial de concepção e arquitetura de sistemas, softwares ou infraestruturas, em vez de tratá-la como um ajuste posterior.

**Segregação de Função (SoD)**: ou Segregation of Duties é um controle interno que divide responsabilidades e tarefas críticas entre diferentes pessoas para prevenir fraudes e erros, garantindo que uma única pessoa não tenha o controle total sobre um processo.

**Segurança da Informação (SI):** Conjunto de práticas, tecnologias e políticas projetadas para proteger dados tanto digitais quanto físicos contra acessos não autorizados, uso indevido, alterações, roubo ou destruição.

**Senha**: É uma sequência de caracteres que é usada para autenticar a identidade de um usuário em um sistema de computador, aplicação ou em um site.

**SIEM (Security Information and Event Management):** Solução de cibersegurança que coleta, centraliza e analisa dados de log de diversas fontes da rede em tempo real.

**Sistemas**: São considerados dentro do escopo todos os programas, sistemas, aplicações, serviços, infraestruturas e plataformas utilizados pelo Grupo e seus colaboradores para atingir objetivos operacionais ou funcionais. Estão incluídos todos os sistemas que impactam direta ou indiretamente, a operação da empresa e que sejam utilizados para fins relacionados às suas atividades, especialmente aqueles que exigem autenticação ou autorização de acesso.

**Sistema de Segurança da Informação (SGSI):** Conjunto estruturado de políticas, procedimentos, processos e recursos que uma organização adota para proteger seus ativos de informação.

**SQL (Structured Query Language):** Linguagem de Consulta Estruturada é uma linguagem padrão para interagir com bancos de dados relacionais.

**SOC (System and Organization Controls):** Equipe e um local centralizado (físico ou virtual) focado em monitorar, detectar e responder a incidentes de segurança cibernética em tempo real.

**Software as a Service (SaaS):** Software como Serviço é um modelo de distribuição de software baseado na nuvem, onde aplicativos são acessados

prevent fraud and errors, ensuring that a single person does not have total control over a process.

**Information Security (IS)**: A set of practices, technologies, and policies designed to protect both digital and physical data against unauthorized access, misuse, alteration, theft, or destruction.

**Password:** A sequence of characters used to authenticate a user's identity on a computer system, application, or website.

**SIEM (Security Information and Event Management):** A cybersecurity solution that collects, centralizes, and analyzes log data from various network sources in real time.

**Systems:** All programs, systems, applications, services, infrastructure, and platforms used by the Group and its employees to achieve operational or functional objectives are considered within the scope. This includes all systems that directly or indirectly impact the company's operation and that are used for purposes related to its activities, especially those that require authentication or access authorization.

**Information Security System (ISMS)**: A structured set of policies, procedures, processes, and resources that an organization adopts to protect its information assets.

**SQL (Structured Query Language)**: Structured Query Language is a standard language for interacting with relational databases.

**SOC (System and Organization Controls)**: A team and a centralized location (physical or virtual) focused on monitoring, detecting, and responding to cybersecurity incidents in real time.

**Software as a Service (SaaS)**: Software as a Service is a cloud-based software distribution model where applications are accessed over the internet via a browser, without the need for local installation.

**Regulatory Bodies**: Public entities with administrative and financial autonomy, created by the government to regulate, supervise, and oversee. They establish rules for private companies, ensuring the quality of services, protecting consumers, and promoting competition.

| | |
|---|---|
| pela internet via navegador, sem necessidade de instalação local.<br><br>**Órgãos Reguladores:** Entidades públicas com autonomia administrativa e financeira, criadas pelo governo para normatizar, supervisionar e fiscalizar. Eles estabelecem regras para empresas privadas, garantindo a qualidade dos serviços, protegendo consumidores e promovendo a concorrência.<br><br>**VPN Virtual Private Network**: é um conceito que cria um "túnel" seguro e criptografado entre o dispositivo de um usuário e a Internet, mascarando seu endereço IP e criptografando seus dados para proteger sua privacidade, segurança e autonomia online. | **VPN (Virtual Private Network**): This is a concept that creates a secure, encrypted "tunnel" between a user's device and the internet, masking their address. |
| | |
| **7. Diretrizes Gerais \| *General Guidelines*** | |
| **Interpretação:** Esta Política de Segurança da Informação (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.<br><br>**Publicidade:** Esta PSI e seus documentos complementares devem ser divulgados ao Departamento de Compliance, visando dar publicidade para todos que se relacionam profissionalmente com a Hedgepoint.<br><br>**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 Hedgepoint e devem ser utilizados unicamente para fins profissionais.<br><br>**Classificação da Informação:** Todas as informações de propriedade ou sob a responsabilidade do Grupo Hedgepoint devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida, conforme "Política de Classificação da Informação".<br><br>**Sigilo:** É vedada, a qualquer tempo, a revelação de informação de propriedade ou sob a responsabilidade do Grupo Hedgepoint sem a prévia e formal autorização do Gestor da Informação, excetuando-se a informação 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 | **Interpretation:** This *Information Security Policy* (ISP) and its supporting documents shall be interpreted in a restrictive way, in other words, activities that are not comprised under Hedgepoint's policies and procedures should only be performed after a previous and formal consent from the employee's Manager.<br><br>**Advertising:** This ISP and its supplementary documents should be disseminated to the Compliance Department, aiming to provide publicity to all those who have professional relations with Hedgepoint.<br><br>**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 Hedgepoint Group must be solely used for business purposes.<br><br>**Data Classification:** All information owned by or under the responsibility of the Hedgepoint Group must be classified and protected with specific controls throughout its lifecycle, according to the 'Information Classification Policy'.<br><br>**Confidentiality**: At any time, the disclosure of information owned by or under the responsibility of the Hedgepoint Group without the prior and formal authorization of the Information Manager is prohibited, except for public information. Information is classified as public when it can be disclosed to everyone, that is, employees, interns, visitors, service providers, and the general public, without affecting |

impactos no negócio. Em caso de dúvida quanto a informação, procurar o Gestor imediato.

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

I. **Uso dos Recursos de TI:** Os Recursos de TI de propriedade ou sob a responsabilidade do Grupo Hedgepoint devem ser utilizados somente para fins profissionais.

II. **BYOD (Bring Your Own Device):** A empresa não aprova, como regra geral, a utilização de dispositivos pessoais, para acesso a sistemas corporativos, redes internas, e-mails institucionais ou tratamento de informações da organização. O acesso aos ativos de informação deve ocorrer exclusivamente por meio de dispositivos corporativos devidamente configurados e gerenciados pela área de Tecnologia da Informação. Excepcionalmente, em situações devidamente justificadas por necessidade operacional e formalmente aprovadas pelos Gestores da área solicitante e de Tecnologia da Informação e Segurança da Informação, poderá ser concedida autorização específica para uso de dispositivo pessoal. Nesses casos, o dispositivo deverá atender integralmente aos requisitos mínimos de segurança estabelecidos pela Hedgepoint, incluindo, mas não se limitando a: instalação de ferramentas de gerenciamento e proteção corporativa, configuração de mecanismos de autenticação forte, criptografia, atualização automática de sistemas e softwares, e possibilidade de aplicação de controles de monitoramento e, quando necessário, de bloqueio ou remoção remota de dados corporativos. A autorização será concedida por prazo determinado e poderá ser revogada a qualquer tempo em caso de descumprimento das diretrizes estabelecidas.

III. **Dispositivos Móveis Corporativos:** Os dispositivos móveis devem ser utilizados quando fornecidos ou autorizados previamente pelo Diretor da área e/ou pelos departamentos de RH e Compliance, a depender da necessidade, seguindo as recomendações de utilização de Rede Virtual Privada (VPN), ferramentas de gerenciamento e bloqueio remoto.

the business. Any question regarding data classification must be submitted to the line manager.

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

I. **Usage of IT Resources:** The IT resources of property or under Hedgepoint Group's responsibility shall be used only for business purposes, in accordance with local legislation.

II. **BYOD (Bring Your Own Device):** The company does not approve, as a general rule, the use of personal devices to access corporate systems, internal networks, institutional email, or to handle the organization's information.

Access to information assets must occur exclusively through corporate devices properly configured and managed by the Information Technology area. Exceptionally, in situations duly justified by operational necessity and formally approved by the Managers of the requesting area and of Information Technology and Information Security, specific authorization may be granted for the use of a personal device. In these cases, the device must fully meet the minimum security requirements established by Hedgepoint, including, but not limited to: installation of corporate management and protection tools, configuration of strong authentication mechanisms, encryption, automatic updating of systems and software, and the possibility of applying monitoring controls and, when necessary, blocking or remotely removing corporate data. The authorization will be granted for a specific period and may be revoked at any time in case of non-compliance with the established guidelines.

III. **Corporate Mobile Devices:** mobile devices should be used when provided or previously authorized by the Area Director and/or the HR and Compliance departments, depending on the need, following the recommendations for using a Virtual Private Network (VPN), management tools, and remote locking.

IV. **Assets Inventory:** The Infrastructure IT team maintains an updated hardware and software inventory, including the asset identification and the person responsible for it.

IV. **Inventário dos Ativos:** O Departamento de Infraestrutura de TI mantém de modo atualizado um inventário de hardwares e softwares contendo, no mínimo, as informações necessárias do ativo e colaborador responsável pelo uso.

V. **Repositórios Digitais e Dispositivos Removíveis:** Somente é permitido o uso do Sharepoint autorizado e fornecido pela Hedgepoint para o armazenamento e transmissão de informações de propriedade ou sob a responsabilidade da empresa. É vedado aos colaboradores o uso de repositórios digitais ou dispositivos removíveis não autorizados pela Hedgepoint.

VI. **Aplicativos de Comunicação Instantânea:** Somente é permitido o uso de aplicativos de Comunicação Instantânea autorizados e fornecidos pela Hedgepoint para troca de informações corporativas.

VII. **Uso de Inteligência Artificial (IA):** A utilização de ferramentas e soluções baseadas em Inteligência Artificial (IA), sejam elas corporativas ou públicas, deve observar critérios de segurança da informação, confidencialidade, privacidade e proteção de dados, sendo expressamente vedada a inserção de informações classificadas como confidenciais, restritas, estratégicas ou que contenham dados pessoais sensíveis sem autorização formal e avaliação prévia de risco. O uso dessas tecnologias deve estar alinhado às diretrizes internas de governança, gestão de riscos, conformidade regulatória e proteção de dados, sendo obrigatório que colaboradores utilizem apenas ferramentas aprovadas pela área de Tecnologia da Informação e Segurança da Informação. Para orientações detalhadas, responsabilidades, exceções e esclarecimento de dúvidas, deve ser consultado o Procedimento de Uso de Inteligência Artificial.

**Controle de Acesso:** A Hedgepoint gerencia o acesso físico e lógico aos seus ambientes que contenham 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,

V. **Digital repositories and Removable Storage Devices:** only the usage of SharePoint, authorized and provided by Hedgepoint Group, is permitted to store and transmit proprietary information belonging to or under the company's responsibility. The usage of digital repositories or removable devices not authorized by Hedgepoint Group is not permitted.

VI. **Instant Communication Application:** Only the use of Instant Messaging applications authorized and provided by Hedgepoint for the exchange of corporate information is permitted.

VII. **Use of Artificial Intelligence (AI):** The use of tools and solutions based on Artificial Intelligence (AI), whether corporate or public, must observe criteria of information security, confidentiality, privacy, and data protection. The insertion of information classified as confidential, restricted, strategic, or containing sensitive personal data is expressly prohibited without formal authorization and prior risk assessment. The use of these technologies must be aligned with internal guidelines for governance, risk management, regulatory compliance, and data protection. Employees are required to use only tools approved by the Information Technology and Information Security areas. For detailed guidance, responsibilities, exceptions, and clarification of doubts, please consult the Artificial Intelligence Usage Procedure.

**Access Control:** The Hedgepoint Group manages both physical and logical access to its environments containing 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, Hedgepoint uses the criteria of "least privilege access" and "need to know access" to define access levels for each employee, according to Access Management Policy.

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 Hedgepoint 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".

III. Para garantir a autenticidade do acesso aos sistemas lógicos é utilizado múltiplo fator de autenticação nos sistemas, quando aplicável.

IV. É responsabilidade dos Gestores das áreas de negócio, e quando necessário do proprietário do(s) sistema(s) definir aspectos de perfis adequados às funções executadas pelos colaboradores no acesso ao(s) sistema(s), conforme controle realizado via Matriz de Segregação de Funções (SoD).

**Ambientes Lógicos:** Os sistemas e Recursos de TI que suportam os processos e as informações do Grupo Hedgepoint devem ser confiáveis, íntegros, seguros e disponíveis a quem deles necessitem para execução de suas atividades profissionais. A fim de garantir a segurança acima estabelecida, a Hedgepoint utiliza os seguintes sistemas de proteção, ativos e atualizados:

**I. Hacker Rangers:** Plataforma de treinamento e desenvolvimento de competências em Segurança da Informação (SI), integrada aos programas contínuos de conscientização e capacitação especializada, com o objetivo de fortalecer a cultura de segurança organizacional.

**II. Delinea Secret Server (PAM e Cofre de Senhas):** Solução de Privileged Access Management (PAM) para gerenciamento seguro de credenciais privilegiadas. O cofre de senhas do Delinea garante o armazenamento seguro, controle de acesso e rotação automática de senhas, reduzindo riscos de acessos não autorizados a sistemas críticos.

**III. AWS (Web Application Firewall):** Proteção contra-ataques a aplicações web, como injeção de SQL e ataques DDoS, integra-se ao conceito de Security by Design, protegendo sistemas desde sua concepção.

**IV. CrowdStrike:** Detecção avançada de ameaças, monitoramento proativo e atuação direta em EDR (*Endpoint Detection and Response*).

**V. Shodan:** Ferramenta de busca de dispositivos conectados à internet, utilizada para análise de

III. To ensure the authenticity of access to logical systems, multi-factor authentication is used in these systems, when applicable.

IV. It is the responsibility of the Business area Managers, and when necessary, the owner of the system(s) to define aspects of profiles suitable for the functions performed by the employees when accessing the system(s), as controlled through the Segregation of Duties Matrix (SoD).

**Logical Environments:** All systems and resources that support the processes and information from Hedgepoint Group should be reliable, thorough, safe, secure, and available to those who need them to carry their professional activities. To ensure the safety and security set forth above, Hedgepoint Group uses protection systems and keep them active and updated:

**I. Hacker Rangers:** A training platform for developing Information Security (IS) skills, integrated with ongoing awareness programs and specialized training to strengthen the organizational security culture.

**II. Delinea Secret Server (PAM and Password Vault):** A Privileged Access Management (PAM) solution for secure management of privileged credentials. Delinea's password vault ensures secure storage, access control, and automatic password rotation, reducing the risk of unauthorized access to critical systems.

**III. AWS WAF (Web Application Firewall):** Protection against web application attacks such as SQL injection and DDoS attacks, aligned with the Security by Design concept, safeguarding systems from their inception

**IV. CrowdStrike:** Advanced threat detection, proactive monitoring, and direct action in Endpoint Detection and Response (EDR).

**V. Shodan:** A search engine for internet-connected devices used for vulnerability analysis and continuous assessment of asset exposure.

**VI. ManageEngine Endpoint Central:** Centralized device management and endpoint security.

vulnerabilidades e suporte em avaliações contínuas de exposição de ativos**.**

**VI. ManageEngine Endpoint Central:** Gestão centralizada de dispositivos e segurança de endpoints.

**VII. Netskope:** Proteção de dados na nuvem (CASB), controle de acesso e prevenção contra vazamento de dados, alinhado ao Data Loss Prevention (DLP) e integrado com SIEM para monitoramento do ambiente.

**VIII. SIEM as a Service:** Centralização de logs e eventos de segurança, com detecção automatizada de incidentes.

**IX. Sistema de AntiSpam:** Implementação de solução avançada de filtragem de e-mails para prevenir ameaças como phishing, malware e spam, assegurando a integridade das comunicações e mitigando riscos de comprometimento por ataques direcionados.

**Desenvolvimento e Aquisição de Software:** Tanto o desenvolvimento interno e externo de softwares como aquisições de mercado devem cumprir os requisitos de segurança da informação e controles de acesso previstos nesta PSI e demais Políticas Complementares, este processo vale também para "software as a service" (SaaS). Antes do desenvolvimento e/ou aquisição de softwares os Departamentos de Infraestrutura de TI e de Segurança Cibernética devem ser consultados.

Para garantir a integridade e a segurança de nossos sistemas e dados, é imprescindível que o Departamento de TI seja consultado previamente, via cybersecurity@hedgepointglobal.com, à fase de desenvolvimento ou aquisição de quaisquer soluções de Computação de Usuário Final (EUC - End-User Computing). Esta consulta deve seguir as diretrizes da Política de Desenvolvimento de Sistemas, Projetos e Inovações.

Toda aquisição de software, plataformas ou qualquer recurso tecnológico, deverá obrigatoriamente passa pelo fluxo e aprovação de compras conforme seu processo e sistema vigente.

Fica expressamente proibida a publicação, disponibilização ou exposição na internet pública, ou em qualquer rede externa, de ambientes de desenvolvimento, teste, homologação ou prototipagem de sistemas, portais, interfaces, páginas de login ou quaisquer componentes que reproduzam

**VII. Netskope:** Cloud data protection (CASB), access control, and data leakage prevention, aligned with Data Loss Prevention (DLP) and integrated with SIEM for environmental monitoring.

**VIII. SIEM as a Service:** Centralized logging and security event management with automated incident detection.

**IX. Anti-Spam System:** Implementation of an advanced email filtering solution to prevent threats such as phishing, malware, and spam, ensuring the integrity of communications and mitigating the risk of compromise from targeted attacks.

**Software Development and Acquisition:** both internal and external software development, including purchases from the market, must comply with the data security requirements and access controls set in the ISP, and in any other Complementary Procedures, this process also applies to software as a service (SaaS). Before the development and/or acquisition of software, the IT Infrastructure and Cybersecurity departments must be consulted.

To ensure the integrity and security of our systems and data, it is essential that the IT Department is consulted in advance, via cybersecurity@hedgepointglobal.com, before the development or acquisition phase of any End-User Computing (EUC) solutions. This query must follow the guidelines of the Systems, Projects, and Innovations Development Policy.

All acquisitions of software, platforms, or any technological resource must necessarily go through the purchasing flow and approval according to its current process and system.

It is expressly forbidden to publish, make available, or expose on the public internet, or on any external network, development, testing, homologation, or prototyping environments of systems, portals, interfaces, login pages, or any components that reproduce or resemble corporate systems of the Hedgepoint Group, even partially or temporarily, without prior formal authorization from the IT and Cybersecurity Department. Any external exposure of any phase of development requires a security review

| | |
|---|---|
| ou se assemelhem a sistemas corporativos do Grupo Hedgepoint, mesmo que de forma parcial ou temporária, sem prévia autorização formal do Departamento de TI e de Segurança Cibernética. Toda exposição externa de qualquer fase do desenvolvimento exige revisão de segurança e aprovação escrita prévia do Departamento de Segurança Cibernética | and prior written approval from the Cybersecurity Department. |
| **Proibição de Contratação e Uso de Ferramentas e Serviços de Tecnologia Não Homologados (Shadow IT)** | **Prohibition on Hiring and Using Non-Approved Technology Tools and Services (Shadow IT)** |
| É expressamente vedado ao colaborador contratar, adquirir, assinar ou utilizar, por conta própria ou de qualquer outra forma não autorizada, ferramentas, plataformas, aplicativos, serviços em nuvem ou soluções de software — sejam gratuitas ou pagas, independentemente de quem arque com o custo — para uso em atividades profissionais relacionadas ao Grupo Hedgepoint, sem prévia avaliação e aprovação formal pelos Departamentos de TI e de Segurança Cibernética. | It is expressly forbidden for employees to hire, acquire, subscribe to, or use, on their own or in any other unauthorized manner, tools, platforms, applications, cloud services, or software solutions — whether free or paid, regardless of who bears the cost — for use in professional activities related to the Hedgepoint Group, without prior evaluation and formal approval by the IT and Cybersecurity Departments. |
| É igualmente vedado ao colaborador conceder, compartilhar ou distribuir acessos a ferramentas ou plataformas não homologadas pela Hedgepoint a outros colaboradores, estagiários, prestadores de serviços ou qualquer terceiro, ainda que a ferramenta tenha sido contratada com recursos pessoais do próprio colaborador. | It is equally forbidden for the employee to grant, share, or distribute access to tools or platforms not approved by Hedgepoint to other employees, interns, service providers, or any third party, even if the tool was contracted using the employee's own personal resources. |
| O uso de recursos pessoais para custear a contratação de tecnologias de uso corporativo não confere ao colaborador qualquer direito de uso, autorização implícita ou isenção das obrigações previstas nesta Política. Toda ferramenta ou serviço tecnológico utilizado no exercício das atividades profissionais, independentemente de sua forma de aquisição ou custeio, está sujeito aos requisitos de segurança da informação estabelecidos pelo Grupo Hedgepoint e deve passar pelo processo formal de homologação antes de qualquer uso. | The use of personal resources to finance the acquisition of corporate-use technologies does not grant the employee any right of use, implicit authorization, or exemption from the obligations set forth in this Policy. All technological tools or services used in the performance of professional activities, regardless of how they are acquired or financed, are subject to the information security requirements established by the Hedgepoint Group and must undergo a formal approval process before any use. |
| Colaboradores que identifiquem necessidade de novas ferramentas ou serviços tecnológicos devem solicitar formalmente a avaliação ao Departamento de TI por meio do endereço cybersecurity@hedgepointglobal.com. O descumprimento desta diretriz caracteriza violação desta PSI e sujeita o colaborador às penalidades previstas no capítulo de Penalidades deste documento. | Employees who identify a need for new technological tools or services must formally request an evaluation from the IT Department via the email address cybersecurity@hedgepointglobal.com. Failure to comply with this guideline constitutes a violation of this Information Security Policy and subjects the employee to the penalties outlined in the Penalties chapter of this document. |
| | **Backup:** the Hedgepoint 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. |

| | |
|---|---|
| **Salvaguarda (backup):** A Hedgepoint 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. | **Monitoring:** Hedgepoint Group monitors its physical and logical environments, aiming at the effectiveness of the implemented controls, the protection of its assets, its reputation, and the identification of events or alerts related to information security incidents. Hedgepoint reserves the right to monitor, audit, and/or inspect at any time and without prior notice or justification, IT resources, as well as to decide on the eventual withdrawal of any usage granted to an employee, without prior notice or justification, whenever deemed necessary. |
| **Monitoramento:** A Hedgepoint 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. A Hedgepoint se reserva ao direito de monitorar, auditar e/ou inspecionar a qualquer momento e sem prévio aviso nem justificativa, os recursos de TI, bem como deliberar por eventual retirada de qualquer uso cedido ao colaborador, sem prévio aviso ou justificativa, sempre que considerar necessário. | Periodic tests and scans for vulnerability detection will be conducted (once a year). |
| Serão realizados periodicamente, ao menos uma vez ao ano testes e varreduras para a detecção de vulnerabilidades. | Hedgepoint continuously monitors activities and analyzes security logs to identify, record, and investigate unauthorized access, breach attempts, and other suspicious activities. This process contributes to the traceability of actions performed on systems, supports audits, and ensures compliance with the Information Security Policy. |
| A Hedgepoint realiza o monitoramento contínuo das atividades e análise de logs de segurança, com o objetivo de identificar, registrar e investigar acessos não autorizados, tentativas de violação e outras atividades suspeitas. Esse processo contribui para a rastreabilidade das ações realizadas nos sistemas, apoio a auditorias e garantia de conformidade com a Política de Segurança da Informação. | **Cyber Risk Management:** The Cybersecurity Department identifies and assesses risks related to IS and Cybersecurity and adopts best practices for its management and control. The "Determination of Cybersecurity Risk" will follow the same risk matrix defined by the Operational Risks area of Hedgepoint Group. |
| **Gestão de Riscos Cibernéticos:** O Departamento de Segurança Cibernética identifica e avalia os riscos relacionados à SI e Cibersegurança e adota as melhores práticas para o seu gerenciamento e controle. A "Determinação Do Risco De Cibersegurança" seguirá a mesma matriz de riscos definida pela área de Riscos Operacionais do Grupo Hedgepoint. | The criteria for accepting cyber risks relate to specific situations where risk response actions are complex or costly to implement compared to the potential effects of the risk, considering all possible impacts and the risk appetite of the Hedgepoint Group, according to the Operational Risk Management Policy. |
| Os critérios para aceitação de riscos cibernéticos, relaciona-se a situações específicas em que as ações de resposta ao risco são complexas ou dispendiosas para implementar em comparação com os possíveis efeitos do risco, considerando todos os impactos possíveis e o apetite de risco do Grupo Hedgepoint, conforme a Política de Gestão de Risco Operacional. | **Change Management:** The progress and outcome of a change, mainly in the systems and infrastructure of the Hedgepoint Group, need to follow the controls related to availability, integrity, confidentiality, and authenticity of the information and are executed only by the IT Department. According to the guidelines of the CAB (Change Advisory Board). |
| **Gestão de Mudança:** O andamento e o resultado de uma mudança, principalmente nos sistemas e na infraestrutura tecnológica do Grupo Hedgepoint, devem preservar os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações e realizados somente pelo Departamento | **Incident Response Plan:** In the event of an Information Security incident that compromises or may compromise the integrity, confidentiality, or availability of systems, infrastructure, data, services, and information assets, the Incident Response Plan must be activated immediately. This plan establishes |

| | |
|---|---|
| de TI, conforme diretrizes do CAB (Change Adivisory Board).<br><br>**Plano de Resposta a Incidentes:** Em caso de incidente de Segurança da Informação que comprometa ou possa comprometer a integridade, confidencialidade ou disponibilidade de sistemas, infraestrutura, dados, serviços e ativos de informação, o Plano de Resposta a Incidentes deve ser acionado imediatamente. Esse plano estabelece procedimentos detalhados de resposta, definição de responsabilidades, tratamento de exceções e orientações para esclarecimento de dúvidas, garantindo uma atuação rápida e adequada diante da situação.<br><br>**Plano de Contingência**: Caso seja identificado um incidente de Segurança da Informação classificado como de alto risco, que ameace a continuidade de serviços essenciais, a segurança de pessoas, a integridade de dados, sistemas ou infraestrutura, bem como em situações de desastres ou emergências, deverá ser adotadas imediatamente medidas alternativas de contingência. Estabelecendo as ações e medidas necessárias para mitigar impactos, assegurar a continuidade das atividades críticas e promover o restabelecimento das operações no menor tempo possível.<br><br>**Continuidade do Negócio:** Os procedimentos de gestão de Continuidade do Negócio devem ser executados em conformidade com a Política de Continuidade de Negócios sob a responsabilidade da área de Riscos Operacionais do Grupo Hedgepoint.<br><br>**Investimentos:** Os investimentos em SI na Hedgepoint são estudados e deliberados pelo Departamento de Segurança Cibernética junto à Diretoria, e quando necessário alinhado com as áreas de negócio, considerando a viabilidade dos investimentos (custo x benefício) e os impactos na qualidade dos processos de negócio.<br><br>**Comitê de Tecnologia, Privacidade e Segurança da Informação (CTPSI):** A Hedgepoint estabeleceu um CTPSI responsável por atuar com independência e objetividade visando o melhor interesse do Grupo Hedgepoint, além de envidar esforços para o desenvolvimento e adoção das boas práticas de Governança Corporativa e negócios.<br><br>É fundamental a participação de representantes de TI e SI, em Comitês de Riscos Operacionais e de Produtos, para analisar se algum assunto tratado nestes Comitês | detailed response procedures, defines responsibilities, handles exceptions, and provides guidance for clarifying doubts, ensuring a rapid and appropriate response to the situation.<br><br>**Contingency Plan**: If a high-risk Information Security incident is identified that threatens the continuity of essential services, the safety of people, the integrity of data, systems or infrastructure, as well as in situations of disasters or emergencies, alternative contingency measures must be adopted immediately and contingency alternatives measures. This involves establishing the necessary actions and measures to mitigate impacts, ensure the continuity of critical activities, and promote recovery as soon as possible.<br><br>**Business Continuity:** The Business Continuity Management procedures must be executed in accordance with the Business Continuity Policy under the responsibility of the Operational Risk area of the Hedgepoint Group.<br><br>**Investments:** The investments are analyzed and decided by the Cybersecurity area together with the Head of IT and, when necessary, they are aligned with the business areas, considering the feasibility of the investment (cost/benefit) and its impacts on the quality of the business processes.<br><br>**Technology, Privacy and Information Security Committee (TPISC)**: Hedgepoint Group set an Information Security Committee responsible for acting, independently and objectively, in the best interests of Hedgepoint Group, such committee is also responsible for the development and adoption of best practices in Corporate and Business Governance.<br><br>It is essential for representatives from IT and IS to participate in Operational Risk and Product Committees, to analyze if any topic discussed in these Committees requires assessments in the SI and/or IT aspect.<br><br>**Security Incident Reporting and Escalation:** Hedgepoint has a communication channel disclosed to its employees to report potential information security incidents: cybersecurity@hedgepointglobal.com.<br><br>Once a security incident is confirmed, regardless of its classification, it must be registered using the operational risk incident registration form, available on the company intranet at the following address: OPERATIONAL RISK INCIDENT FORM. The escalation |

| | |
|---|---|
| apresenta necessidade de avaliações no aspecto de SI e/ou TI. | of information security incidents follows the guidelines defined in Hedgepoint's Risk Management Escalation Policy. |
| **Comunicação e Escalonamento de Incidentes de Segurança:** A Hedgepoint possui um canal de comunicação divulgado aos seus colaboradores para reportar possíveis casos de incidentes de segurança da informação: cybersecurity@hedgepointglobal.com. Confirmado o incidente de segurança independente de sua classificação, este deve ser registrado através de formulário para registro de incidentes relacionados a riscos operacionais, disponível na intranet da empresa através do seguinte endereço: FORMULÁRIO DE INCIDENTES DE RISCO OPERACIONAL. O escalamento de incidentes de segurança da informação segue as diretrizes definidas na Política de Escalamento de Gestão Riscos da Hedgepoint. | Additionally, any cyber incident and/or personal data breach must be formally reported to the Compliance and DPO/Legal area immediately upon confirmation, which will be responsible for coordinating the regulatory assessment and, when applicable, ensuring reporting to the competent regulatory bodies within the established deadlines, in accordance with current legislation and applicable regulations. For the external public, the channel csirt@hedgepointglobal.com is provided for reporting any cybersecurity-related issues. |
| Adicionalmente, todo incidente cibernético e/ou vazamento de dados pessoais deverá ser formalmente comunicado à área de Compliance e DPO/Legal imediatamente após sua confirmação, a qual será responsável por coordenar a avaliação regulatória e, quando aplicável, assegurar o reporte aos órgãos reguladores competentes nos prazos estabelecidos, em conformidade com a legislação vigente e normativos aplicáveis. | **Personal Data Protection:** Hedgepoint group respects 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. |
| Para o público externo é disponibilizado o canal csirt@hedgepointglobal.com para o reporte de qualquer questão relacionada à cibersegurança. | **Training:** Hedgepoint establishes a periodic and annual training plan aimed at the development, awareness, and maintenance of the skills of employees in Cybersecurity. These trainings are mandatory and is carried out at the beginning of each year, and the completion results will be assessed by the HR department. |
| **Proteção de Dados Pessoais:** A Hedgepoint 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. | **Review and Update:** Hedgepoint Group keeps a program to review and update this ISP and the Complementary Policies whenever needed, provided that it does not exceed the maximum period of 12 (twelve) months, to ensure that all security and legal technical requirements are implemented and up to date. |
| **Capacitação:** A Hedgepoint estabelece um plano periódico e anual de capacitação direcionado ao desenvolvimento, conscientização e manutenção das habilidades dos colaboradores sobre Segurança Cibernética. Estes treinamentos têm caráter obrigatório, sendo realizado todo início de cada ano, e os resultados de conclusão serão auferidos pelo departamento de RH. | **Changes:** Changes to this Information Security Policy should be made by the Cybersecurity team. Changes to the Supplementary Policies must be duly communicated to the Cybersecurity Department through the email address: cybersecurity@hedgepointglobal.com. |
| **Revisão e Atualização:** A Hedgepoint possui e mantem um programa de revisão/atualização desta PSI e das Políticas Complementares sempre que se fizer necessário, desde que não exceda o período máximo de 12 (dozes) meses, visando à garantia que todos os requisitos de segurança técnicos e legais | **Exceptions:** Can only be permitted on circumstances that are considered exceptions to this ISP, they should be temporary and approved in advance by the Head of the area and Head of IT, Cybersecurity Manager and/or IT Head to have an effect, in addition, they may be |

| | |
|---|---|
| implementados estejam sendo cumpridos e atualizados.<br><br>**Alterações:** As alterações desta PSI devem ser feitas pelo time de Segurança Cibernética, alterações nas Políticas Complementares devem ser devidamente comunicadas ao Departamento de Segurança Cibernética, por meio do endereço eletrônico: cybersecurity@hedgepointglobal.com.<br><br>**Exceções:** As exceções somente são admitidas de forma excepcional a essa PSI, devendo ser temporárias e aprovadas previamente pelo Head da respectiva área, Gerente de Segurança Cibernética e/ou CTO para produzirem efeito, além disso, podem ser revogadas a qualquer tempo por mera liberalidade do Gestor do colaborador ou do Head da área, sem aviso prévio.<br><br>**Dúvidas:** Qualquer dúvida relativa a esta PSI deve ser encaminhada ao Departamento de Segurança Cibernética por meio do endereço eletrônico: cybersecurity@hedgepointglobal.com. | revoked at any time, by decision of the employee's manager or by the Head of IT, without prior notice.<br><br>**Questions:** Any questions regarding this ISP must be submitted to the Cybersecurity Department through the e-mail address: cybersecurity@hedgepointglobal.com. |
| | |
| **8. Penalidades \| *Penalties*** | |
| I. **Violações:** Qualquer atividade que desrespeite as disposições estabelecidas nesta Política ou em quaisquer das Políticas Complementares do Grupo Hedgepoint deve ser considerada como uma violação e tratada, a fim de apurar as responsabilidades dos envolvidos de acordo com as "Medidas Disciplinares", visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente;<br><br>II. **Tentativa de Burla:** A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação. | I. **Violations:** any activity that violates the rules established in this policy or in any of the complementary policies of the Hedgepoint Group must be considered a violation and the involved parties will be subject to "disciplinary measures". In this case, contractual and legal sanctions might be applied.<br><br>II. **Attempt of Fraud:** When detected, an attempt to bypass established guidelines and controls should be treated as a violation. |
| | |
| **9. Considerações Finais \| *Final Considerations*** | |

| | |
|---|---|
| I. Esta Política deve ser revisada, no mínimo, a cada 12 (doze) meses, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais políticas específicas do Grupo Hedgepoint. | I. This policy should be reviewed at least every twelve (12) months or whenever there is a need for changes on the criteria defined in the other specific policies of the Hedgepoint Group. |
| II. Documentos e arquivos pessoais, não devem ser armazenados nos equipamentos da Hedgepoint. Todos os arquivos hospedados nos bancos de dados ou equipamentos serão considerados dados de propriedade da Hedgepoint, sendo a transferência de arquivos constantemente monitorada. | II. Personal documents and files should not be stored on Hedgepoint equipment. All files hosted on our databases or equipment will be considered property of Hedgepoint, with file transfers being constantly monitored. |
| III. Este documento, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Departamento de Segurança Cibernética. | III. This document and the other documents that complement it are available on the intranet or, in case of unavailability, can be requested to the Cybersecurity Department. |
| IV. Consideramos evento de incidente operacional, qualquer situação que tenha ocorrido e que possa ocasionar problemas na execução dos processos relacionados a esta Política Corporativa. São exemplos de Eventos de Incidente Operacional: indisponibilidade de sistemas, problemas na integridade da informação, erros de digitação e outros. Todo evento deverá ser reportado, independente da sua correlação com perda financeira, ao Gerente responsável pelo processo e as Áreas de Compliance e Risco para o adequado tratamento, classificação e eventual reporte em níveis de alçada superior. | IV. We consider an operational incident event, any situation that has occurred and that may cause problems in the execution of the processes related to this Corporate Policy. Examples of Operational Incident Events are system unavailability, information integrity issues, typing errors, and others. Every event shall be reported, despite the consequences of its association with financial loss, to the Manager responsible for the process and to the Compliance and Risk Areas for the appropriate treatment, classification, and eventual reporting at higher levels. |