Versão:	Data de publicação:	Data de revisão:
02	29/03/2017	18/09/2023
Unidade responsável:		**Aprovador por:**
DPO/Área de Segurança da informação e Privacidade		Conselho de Diretores

Sumário

1. Introdução

1.1. Objetivo

A presente Política de Segurança da Informação ("Política" ou "PSI") tem como objetivo estabelecer diretrizes, normas e procedimentos relacionados à Segurança da Informação, em conformidade com as normativas e boas práticas pertinentes e, visando garantir a proteção das informações vinculadas às atividades da H&P e dos projetos atendidos pela empresa frente a ameaças existentes, minimizando riscos ao negócio, clientes, funcionários, parceiros, fornecedores, prestadores de serviços diretos ou indiretos e públicos atendidos pela H&P.

1.2. Abrangência

As regras contidas nesta política devem ser conhecidas e respeitadas por todos os diretores, conselheiros, funcionários, parceiros e prestadores de serviço diretos ou indiretos da H&P, independentemente de seu nível hierárquico.

É desejável que a Política seja conhecida e respeitada pelos clientes e fornecedores da empresa.

1.3. Termos e Definições

Todos os termos e definições serão centralizados no documento "Glossário de Termos e Definições de Políticas da H&P", disponível no diretório do SharePoint **H&P_Docs**.

1.4. Documentos Complementares

- POL003 - Política de Privacidade e Proteção de Dados.
- Glossário de Termos e Definições de Políticas da H&P
- Código de Conduta da H&P

1.5. Localização do Documento

Este documento foi criado, atualizado, aprovado e publicado por meio dos processos oficiais da H&P e pode ser encontrado em sua versão original no diretório do SharePoint **H&P_Docs**.

2. Princípios de Segurança da Informação

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização, seus clientes e públicos atendidos. Ela pode estar guardada para uso restrito ou exposta às partes interessadas para a consulta ou manuseio. Pode estar impressa ou escrita, pode ser falada, transmitida por e-mails ou outros meios eletrônicos, independentemente da forma apresentada ou o meio pelo qual a informação é compartilhada ou armazenada.

A informação é um importante ativo para a H&P, seus clientes, parceiros e públicos, sendo, portanto, essencial ao negócio desenvolvido pela empresa. Por esse motivo, deverá ser devidamente protegida e utilizada de modo ético e seguro, garantindo confiabilidade por meio da proteção da:

a) **Confidencialidade:** Garantir que a informação não seja revelada ou esteja disponível para indivíduos, entidades e processos não autorizados;

b) **Integridade:** Garantir a salvaguarda da exatidão e totalidade da informação e dos métodos de processamento;

c) **Disponibilidade:** Garantir que a informação esteja sempre acessível e disponível quando necessária.

3. Diretrizes de Segurança da Informação

Para endereçar todo o esforço e manutenção necessária para a Segurança da Informação, a H&P estabelece as seguintes diretrizes:

i. **SGPI:** um processo de Gestão da Privacidade da Informação deve ser estabelecido e mantido com apoio do Conselho de Diretores, por meio de um Sistema de Gestão de Segurança da Informação (SGPI), que envolve as políticas, normas, procedimentos, recursos, indicadores e outras ações direcionadas a esta finalidade.

ii. **Melhoria contínua:** deve-se garantir a melhoria contínua do Sistema de Gestão da Segurança da Informação (SGPI), com base na norma ISO/IEC 27001:2022, ou versão mais atual, contendo todos os indicadores e métricas para monitorar-se o ciclo PDCA.

iii. **Comportamento ético:** toda informação deve ser utilizada com senso de responsabilidade e de modo ético e seguro por todos, em benefício exclusivo dos negócios corporativos, conforme previsto no Código de Conduta da H&P.

iv. **Gestão de ativos:** os ativos tangíveis e intangíveis de informação devem estar identificados de forma individual, inventariados, protegidos e monitorados contra acessos indevidos. As mídias devem ser gerenciadas de forma adequada, conforme os requisitos de segurança da informação previstos nesta ou em norma(s) específica(s).

v. **Uso aceitável dos ativos:** as restrições do uso de ativos na organização, bem como a forma adequada de utilizá-lo, devem ser definidas na extensão considerada pela governança de Segurança da Informação como necessária.

vi. **Gestão de identidades:** a identificação de cada funcionário e prestador de serviços da H&P é única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

vii. **Gestão de acessos:** o controle de acesso dos funcionários, prestadores de serviço, parceiros e fornecedores aos ativos de informação deve ser devidamente aprovado pelo responsável, respeitando norma(s) específica(s) de Segurança da Informação, quer seja para simples consulta ou para alteração.

viii. **Suporte remoto de TI:** concessão de acesso remoto aos funcionários e prestadores de serviço deve ser previamente solicitada e autorizada pela área responsável, conforme previsto em norma(s) específica(s) da H&P.

ix. **Uso de domínio:** o uso do e-mail sob o domínio "@hep.solutions" será permitido apenas para funcionários, prestadores de serviços e parceiros da H&P.

x. **Gestão de riscos:** todos os riscos deverão ser analisados, classificados e apresentados a um comitê que deliberará sobre o tratamento adequado para tais. Os riscos devem ser identificados por meio de um processo estabelecido para análise de causas e possíveis consequências sobre os processos em aspectos de segurança da informação (confidencialidade, integridade e disponibilidade).

xi. **Gestão de incidentes:** todos os incidentes de segurança da informação e privacidade devem ser reportados ao DPO e Área de Segurança da Informação e Privacidade, via formulário do **GLPI - Solicitação GRC** e/ou por outro meio mais eficiente para célere comunicação, para que sejam analisados, avaliados e tratados.

xii. **Conformidade:** a H&P deve identificar, seguir, documentar e manter atualizadas as leis que regulamentam suas atividades, bem como aspectos de propriedade intelectual. Deve-se definir regras para garantir que não ocorram violações jurídicas, regulamentares ou contratuais nos requisitos de segurança da informação na organização.

xiii. **Objetivos estratégicos de segurança da informação:** a H&P, por meio de seu Conselho de Diretores, deve definir os Objetivos Estratégicos de Segurança da Informação considerando esta política, os requisitos de Segurança da Informação aplicáveis e os resultados da gestão de riscos.

xiv. **Responsabilidade dos envolvidos:** todos os funcionários, prestadores de serviço, parceiros e fornecedores que tenham acesso a informações da H&P, bem como de seus clientes e parceiros, devem aderir formalmente ao "Termo de Confidencialidade e Ciência da PSI", anexo deste documento, comprometendo-se a respeitar integralmente esta política e as normas que a suportam.

xv. **Backup:** cópias de segurança devem ser realizadas e testadas, obrigatoriamente para as informações que são consideradas vitais para os sistemas da empresa e para a retomada das atividades da área em caso de contingência.

xvi. **Desenvolvimento Seguro:** regras para o desenvolvimento seguro de sistemas devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

xvii. **Dispositivos móveis:** dispositivos móveis corporativos devem ser destinados ao uso em serviço, mediante autorização prévia com definição de prazo, para a realização das atividades de trabalho e para a comunicação com a empresa, funcionários, prestadores de serviço, fornecedores, clientes e públicos atendidos pela empresa, devendo ser utilizados somente para tais finalidades.

xviii. **Classificação da Informação:** as informações devem ser classificadas e manuseadas de acordo com a confidencialidade e as proteções necessárias, da seguinte forma: Pública, Interna, Restrita e Confidencial. Qualquer tratamento da informação deve levar em consideração a classificação para a devida aplicação de medidas de segurança.

xix. **Criptografia:** um conjunto de regras deve garantir a padronização das técnicas criptográficas, a aplicação adequada destas e as responsabilidades para manter a segurança no transporte ou armazenamento das informações, independentemente do meio utilizado. Quanto à transmissão de informações, esse recurso deve ser utilizado, quando

necessário, para garantir a privacidade na comunicação dos dados da H&P e de seus clientes.

xx. **Gestão de mudanças:** um processo de gestão de mudanças deve ser aplicado para garantir que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, a fim de não ocasionar falhas de confidencialidade, integridade e/ou disponibilidade.

xxi. **Acesso físico:** para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso físico não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho, devem ser adotadas medidas (controles) de segurança.

xxii. **Conscientização e educação:** deve-se garantir que os funcionários, prestadores de serviço e demais partes interessadas, quando pertinente, sejam conscientizados e treinados nas práticas e diretrizes de segurança da informação da organização provenientes desta ou de outras normas específicas do SGPI.

xxiii. **Exceções:** quando, por razões tecnológicas ou determinações superiores, tornarem impossível a aplicação dos requisitos previstos nesta política, o responsável e/ou solicitante deverá reportá-las imediatamente ao DPO por meio do endereço de e-mail privacidade@hep.solutions, para que a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

4. Comunicação e Treinamento

A H&P manterá um plano de comunicação e treinamento periódico proposto pelo Núcleo de Segurança da Informação do que comunicar; quando comunicar; com quem comunicar e como se comunicar inerente ao SGPI, com intuito de divulgar e conscientizar da importância do cumprimento das regras de Segurança da Informação.

5. Governança do SGPI

Para implantar e manter as diretrizes aqui documentadas, bem como a implantação de normas específicas que complementarão as diretrizes e a estrutura de governança do SGPI, o Conselho de Diretores determinou a constituição formal de um Comitê Multidisciplinar de Segurança da Informação e Privacidade (CINF).

Além disso, também é designado o Encarregado pelo Tratamento de Dados (DPO), bem como Núcleo de Segurança da Informação e Privacidade, que conta com profissional dedicado à Segurança da Informação da H&P.

6. Monitoramento e Auditoria

A H&P reserva-se o direito de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto, a organização mantém controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgou necessários para reduzir os riscos, e reserva-se o direito de:

i. **Sistemas de monitoramento:** implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correios eletrônicos, navegação, internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados para fins de mitigar riscos ou fornecer evidências a autoridades competentes.

ii. **Inspeção de dados:** inspecionar qualquer arquivo que esteja na rede, no disco local da estação de trabalho ou qualquer outro ambiente da H&P, visando assegurar o rígido cumprimento desta política.

iii. **Prevenção:** instalar outros sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.

7. Consequências de Violações

Para toda e qualquer infração à PSI e às Normas de Segurança da Informação que a suportam, deverá ser aberto um incidente de segurança da informação, tratado de acordo com o processo de gestão de incidentes de segurança da informação e informado ao DPO e ao Conselho de Diretores. Por conseguinte, o incidente será apurado por meio de procedimentos internos que devem ser conduzidos pela área de Governança, Riscos e Compliance (GRC) em conjunto com a Área de Segurança da Informação e Privacidade da H&P.

Caso o Conselho de Diretores julgue cabível, o funcionário, prestador de serviço, fornecedor ou parceiro envolvido poderá, enquanto durar o processo de apuração interna, ser afastado da função ou ter o contrato suspenso.

A H&P exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos ativos de informação concedidos aos seus funcionários, prestadores de serviços, fornecedores e parceiros para suas atividades, reservando-se o direito de aplicar as medidas disciplinares cabíveis de acordo com a gravidade da violação, de forma justa e proporcional após a análise de dados e evidências nos processos investigatórios e nos casos necessários, adotar as medidas legais cabíveis.

Revisado por:

GUILHERME ANDRADE SILVEIRA:10752652664

Assinado de forma digital por GUILHERME ANDRADE SILVEIRA:10752652664
Dados: 2023.09.22 14:59:06 -03'00'

DPO/Área de Segurança da Informação e Privacidade:

Anexos

Anexo 1. Histórico de Alterações

Data	Revisão	Descrição	Revisado Por
29/03/2017	**00**	Versão Inicial da PSI	-
30/06/2021	**01**	Revisão Integral da PSI	Comitê de Informação e Privacidade
18/09/2023	**02**	Revisão Integral da PSI	DPO/Área Segurança da Informação e Privacidade.

Anexo 2. Termo de Confidencialidade e Ciência da PSI

Informo para devidos fins que li e entendi o documento chamado "Política de Segurança da Informação", também referido no âmbito desta organização como "PSI" e me comprometo em sempre estar atento às atualizações desta política e das normas que a suportam.

Estou ciente que todos os ambientes da H&P, físicos e eletrônicos, como contas de e-mail fornecidas pela empresa, acesso à internet, dispositivos móveis, estão sujeitos a monitoramento para a devida proteção e guarda dos ativos da empresa, seja com uso de câmeras com captação de imagem e voz, seja com uso de dispositivos de autenticação de identidade ou softwares de segurança da informação, para auditorias físicas e/ou eletrônicas. Para tanto, a H&P respeitará as legislações vigentes.

Assumo o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, interna, confidencial ou restrita, que tenha ou venha a ter conhecimento em razão de minhas funções na H&P, mesmo depois de terminado meu vínculo contratual mantido com a organização.

Estou ciente e de acordo que o não cumprimento das condições estabelecidas neste termo poderá culminar no exame da conduta sob o aspecto disciplinar segundo o Código de Conduta da H&P, reparações de natureza civil e criminal, sem prejuízo da rescisão do contrato de trabalho por justa causa, se apurada minha responsabilidade.

Declaro neste ato que comunicarei ao DPO e Área de Segurança da Informação e Privacidade, por meio do endereço de e-mail privacidade@hep.solutions, Canal Confidencial ou via GLPI, todas as irregularidades porventura ocorridas no uso dos recursos tecnológicos e no manuseio de informações, bem como qualquer suspeita ou ameaça ao sigilo e à segurança das informações que eu detectar, para que seja providenciada a imediata regularização e sua averiguação.

Este Termo de Compromisso assinado por mim passa a integrar meu contrato de trabalho

Nome Completo/Razão Social	
CPF ou CNPJ	
Área	
Data	
Assinatura	