1.0 OBJETIVO

Esta política visa estabelecer as medidas técnicas, administrativas e de segurança adotadas pela **Hexágono Engenharia** para proteção dos dados pessoais e organizacionais. Ademais, estabelece diretrizes claras e específicas para garantir que colaboradores, terceiros, fornecedores ou qualquer outra parte relacionada à **Hexágono Engenharia** atue em conformidade com a lei geral de proteção de dados, de acordo com as diretrizes específicas de segurança da informação e em consonância com as exigências do negócio e as demais leis aplicáveis, de forma a preservar tanto os interesses da empresa quanto os direitos individuais dos envolvidos.

É também objetivo dessa política orientar a definição de normas e procedimentos específicos de segurança da informação, além de promover a implementação de controles e processos adequados para assegurar a integridade, confidencialidade e disponibilidade das informações da **Hexágono Engenharia.** Por meio desta política, buscamos garantir que:

1. A **integridade** das informações seja preservada, garantindo que permaneçam em seu estado original e protegendo-as contra alterações indevidas, intencionais ou acidentais durante sua guarda ou transmissão.
2. A **confidencialidade** das informações seja mantida, permitindo o acesso somente a pessoas autorizadas, protegendo-as contra divulgação não autorizada ou uso inadequado.
3. A **disponibilidade** das informações seja garantida, possibilitando que usuários autorizados obtenham acesso aos dados e ativos correspondentes sempre que necessário, de forma a manter a continuidade das operações e dos processos de negócio.

Por fim, a Política de Segurança da Informação (PSI) aqui apresentada também é fundamentada nas diretrizes delineadas pela norma ABNT NBR ISO/IEC 27002:2005, amplamente reconhecida internacionalmente como um referencial de boas práticas para a administração da segurança da informação. Esta norma estabelece um conjunto abrangente de controles e diretrizes destinados a garantir a proteção dos ativos de informação contra ameaças internas e externas.

Ao alinhar nossa PSI com os padrões estabelecidos pela ISO/IEC 27002:2005, buscamos assegurar uma abordagem consistente e eficaz sobre o tema, visando mitigar riscos e fortalecer nosso ambiente físico e digital.

2.0 TERMOS E DEFINIÇÕES

2.1 Backups: Cópias de segurança dos dados ou informações importantes, geralmente armazenadas separadamente para proteger contra perdas de dados causadas por falhas, erros humanos, ou desastres naturais.

2.2 Código de Conduta: Conjunto de princípios, valores e normas que regem as relações da **Hexágono Engenharia** com todas as partes interessadas.

2.3 Datacenter: Local físico onde estão concentrados os recursos de computação, como servidores, armazenamento de dados, e redes, geralmente utilizado para hospedagem e processamento de dados em larga escala.

2.4 Fornecedor: toda pessoa física ou jurídica que forneça insumo, material ou serviço para a **Hexágono Engenharia**.

2.5 Mail bombing: Enviar uma grande quantidade de e-mails para uma única pessoa ou sistema, sobrecarregando o sistema alvo e potencialmente causando interrupções ou danos.

2.6 Ouvidoria: Meio oficial de comunicação disponível para o registro de dúvidas, reclamações, elogios e denúncias sobre potenciais desvios cometidos.

2.7 Parceiro: pessoa física ou jurídica com a qual a Empresa mantenha relação formalizada por meio de acordos, contratos, convênios ou instrumentos similares.

2.8 Partes interessadas: Pessoas físicas ou jurídicas que são diretas ou indiretamente afetadas pelas atividades da **Hexágono Engenharia** e que possuem algum relacionamento com ela (colaboradores, fornecedores, agentes do governo, comunidade, entre outros).

2.9 Phishing: ataque cibernético em que os invasores tentam enganar os usuários para que revelem informações confidenciais, como senhas, dados financeiros ou informações pessoais, geralmente por meio de e-mails, mensagens instantâneas ou páginas da web falsas.

2.10 Spam: Mensagens eletrônicas não solicitadas, geralmente enviadas em massa, com o objetivo de fazer propaganda, espalhar malware ou fraudar.

2.11 Softwares: Programas de computador ou conjunto de instruções que permitem que um computador realize tarefas específicas, como processamento de texto, navegação na web, ou jogos.

2.12 Stakeholders: Indivíduos, grupos ou organizações que têm interesse, direta ou indiretamente, em uma empresa, projeto, ou questão, e podem ser afetados pelas decisões ou ações relacionadas a esse contexto.

2.13 Privacy by Design: É um princípio que visa garantir a proteção de dados pessoais desde a concepção de produtos, serviços e processos, integrando medidas de privacidade e segurança de forma proativa. Esse conceito exige que, em todas as fases de desenvolvimento e operação, a privacidade seja tratada como prioridade, implementando salvaguardas técnicas e organizacionais adequadas para minimizar o

risco de violações e assegurar o cumprimento das legislações aplicáveis, como a LGPD.

3.0 DOCUMENTOS RELACIONADOS

POL-COM-004 - Código de Conduta

POL-COM-010- Política de Gestão da Consequência

POL-COM- 013 - Política de Privacidade

POL-COM-014 - Política de Gestão de Dados.

4.0 PÚBLICO-ALVO

Este documento é aplicável aos colaboradores, diretores e outros públicos de interação com a **Hexágono Engenharia** como prestadores de serviços, fornecedores, parceiros, terceiros e demais partes interessadas pertinentes.

5.0 RESPONSABILIDADES

As diretrizes delineadas neste documento devem ser seguidas por todas as partes vinculadas à **Hexágono Engenharia** e abrangem todas as informações da empresa, independentemente do meio ou formato em que se apresentem.

Além disso, é responsabilidade de cada colaborador manter-se atualizado sobre esta Política de Segurança da Informação (PSI) e os procedimentos correlatos, procurando orientação de seu gestor ou da Gerência de TI sempre que surgirem dúvidas quanto à aquisição, utilização ou descarte de informações. A disponibilização da Política na rede

para que todos tenham acesso é de responsabilidade do Coordenador da Qualidade ou colaborador designado do setor.

Além disso, é de responsabilidade do departamento de Recursos Humanos incluir em todos os contratos de trabalho da **Hexágono Engenharia** o anexo do Termo de Sigilo e Confidencialidade (FO-GEP-019). A atribuição de responsabilidades de cada indivíduo em relação à segurança da informação deve ser claramente comunicada durante o processo de contratação dos colaboradores. Todos os colaboradores devem ser devidamente instruídos sobre os procedimentos de segurança, assim como sobre a utilização adequada dos ativos, visando à mitigação de possíveis riscos.

Ademais, cabe à empresa disponibilizar as diretrizes de segurança da informação tanto no Termo de Responsabilidade pela Guarda e Uso do Equipamento (FO-SGI-022) quanto no Manual do Colaborador (OD-COM-001). Por sua vez, compete ao setor de Suprimentos inserir as Cláusulas de LGPD e adoção de medidas adequadas de segurança da informação em outros contratos com parceiros e prestadores de serviço, sendo essa uma condição essencial para o acesso aos ativos de informação fornecidos pela empresa.

5.1 Responsabilidades específicas dos colaboradores e terceiros

Cada colaborador e terceiro será integralmente responsável por qualquer prejuízo ou dano causado à **Hexágono Engenharia** e/ou a outras partes relacionas resultante da não conformidade com as diretrizes e normas estabelecidas neste documento.

5.2 Responsabilidade específicas dos gestores

a. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
b. Antes de conceder acesso às informações da empresa, verificar se o colaborador está ciente sobre suas responsabilidades.

c. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

5.3 Responsabilidade específicas dos custodiantes da informação

a. Da área de Tecnologia da Informação

A área de Tecnologia da Informação (TI) da **Hexágono Engenharia** possui responsabilidades essenciais para garantir a segurança e integridade dos dados e sistemas da empresa. Isso inclui:

I. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a empresa;

II. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

III. Garantir que, ao ocorrer movimentação interna dos ativos de TI, as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

IV. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;

V. Atribuir a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação um responsável identificável como pessoa física:

• Os usuários individuais de funcionários serão de responsabilidade do próprio funcionário.

• Os usuários de terceiros serão de responsabilidade do gestor da área contratante.

VI. Proteger continuamente todos os ativos de informação da empresa contra código malicioso e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;

VII. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, com auditoria de código e proteção contratual para controle e responsabilização no caso de uso de terceiros;

VIII. Responsabilizar-se pelo uso, manuseio e guarda de assinatura e certificados digitais;

IX. Garantir, mediante solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, férias, incidente, investigação ou outra situação que exija medida restritiva para salvaguardar os ativos da empresa;

X. Assegurar que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro;

XI. Monitorar o ambiente de TI, gerando indicadores e históricos de:

• Uso da capacidade instalada da rede e dos equipamentos.

• Tempo de resposta no acesso à internet e aos sistemas críticos da empresa.

• Períodos de indisponibilidade no acesso à internet e aos sistemas críticos.

• Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, etc.).

• Atividade de todos os colaboradores durante os acessos às redes externas, incluindo internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

5.4 Do Comitê de Governança de Dados

Deve ser formalmente constituído por colaboradores nomeados pela Diretoria para participar do grupo pelo período de dois anos. Deverá o Comitê reunir-se formalmente pelo menos uma vez a cada dois meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a **Hexágono Engenharia**.

Ademais, o Comitê contará com a presença de consultores externos especializados e necessariamente de membro do setor de Tecnologia da Informação para fornecer apoio em questões que demandem conhecimento técnico específico. Sendo assim, é de responsabilidade do Comitê de Governança de Dados:

I. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da **Hexágono Engenharia.**

II. Propor as metodologias e os processos específicos para a segurança da informação como avaliação de riscos inerentes ao modelo de negócio da **Hexágono Engenharia**.

III. Revisar a PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Governança de Dados

IV. Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da **Hexágono Engenharia**, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

V. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

VI. Analisar criticamente incidentes em conjunto com o setor de tecnologia da informação.

VII. Apresentar as atas das reuniões do Comitê de Governança de Dados bem como as principais ações realizadas de forma periódica para a Diretoria.

5.4 Do Encarregado de Dados

O Encarregado de Dados é a pessoa, física ou jurídica, responsável por atuar como canal de comunicação entre a **Hexágono Engenharia**, os titulares de Dados e a Agência Nacional de Proteção de Dados (ANPD). Aqui, esse papel é exercido pela terceirizada "Efetive – Ética e Desenvolvimento Humano".

A Efetive é encarregada de monitorar a conformidade com as leis de privacidade de dados, coordenar treinamentos internos sobre proteção de dados, responder às solicitações dos titulares de dados e garantir que as operações de processamento de dados sejam realizadas de acordo com os princípios de privacidade e segurança da informação.

A empresa terceirizada atua como um parceiro estratégico na implementação e manutenção das políticas de privacidade e segurança de dados da **Hexágono Engenharia**, assegurando o cumprimento das regulamentações e a proteção dos dados dos colaboradores e clientes.

06. DIRETRIZES

6.1 Diretrizes Gerais

É imprescindível que cada membro da equipe esteja ciente de que os ambientes, sistemas, computadores e redes da empresa são monitorados e registrados, em conformidade com as leis brasileiras e mediante prévia comunicação realizada na admissão com a assinatura do Código de Conduta. Somado a isso, destaca-se que:

Propriedade da informação: Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela **Hexágono Engenharia** pertence à referida empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Uso pessoal dos recursos: Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos não é permitido.

Registro de Uso dos Sistemas e Serviços: A **Hexágono Engenharia**, por meio da Gerência de TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Qualquer incidente que comprometa a segurança da informação deve ser relatado inicialmente à Gerência de TI. Esta, após as devidas providências preliminares, encaminhará o incidente ao Comitê de Governança de Dados para análise e controle subsequentes.

Além disso, é imprescindível que os responsáveis por novos projetos dentro da **Hexágono Engenharia** incorporem o conceito de 'Privacy by Design' em todas as suas etapas. Isso significa que desde o planejamento até a execução, deve-se considerar ativamente a proteção dos dados pessoais como um elemento fundamental, garantindo que as medidas de segurança e privacidade sejam integradas de forma intrínseca em cada fase do desenvolvimento do projeto.

Na **Hexágono Engenharia**, estabelecemos diretrizes gerais para a classificação da informação, visando garantir sua confidencialidade, integridade e disponibilidade. Essa classificação é essencial para identificar e categorizar os dados com base em seu valor e sensibilidade, permitindo a aplicação de controles de segurança adequados.

CLASSIFICAÇÃO	CRITÉRIOS	PÚBLICO(S)	EXEMPLO(S)
CONFIDENCIAL	Informações de caráter estratégico de negócios. A informação confidencial é restringida dentro da organização e protegida de acesso externo. Qualquer perda de confidencialidade causará eventual comprometimento das operações, resultando em perdas financeiras, de competitividade, de imagem, risco de ações judiciais à **Hexágono Engenharia** e a seus executivos.	Pessoas elegíveis pelos Diretores da **Hexágono Engenharia**	Atas de reuniões da Diretoria e das reuniões gerenciais.
RESTRITA	Informações de caráter restrito e circulação controlada. Este tipo de informação é de uso restrito a um grupo de pessoas, departamentos específicos, equipes de um projeto etc., divulgada de forma seletiva e mediante o conhecimento e a autorização expressa do proprietário da informação (ex.: informações de projetos, processos etc.).	Somente pessoas elegíveis para tomar conhecimento e uso destas informações.	Fórmulas e ativos protegidos por direito autoral; Assuntos de Comitês; Notas fiscais; Informações pessoais de colaboradores ou outras partes relacionadas à empresa.
INTERNA	Informações de conhecimento e circulação interna. A informação de uso interno é tratada como importante e mantida dentro do domínio **Hexágono Engenharia**, divulgada de forma seletiva e mediante o conhecimento e a autorização expressa do proprietário da informação	Colaboradores e parceiros de negócios que precisam ter conhecimento e uso destas informações.	Comunicações internas; Procedimentos internos, instruções internas.
PÚBLICA	Informações de circulação geral, de conhecimento público. Toda informação que não necessite de sigilo terá livre acesso e não causará qualquer prejuízo para os negócios caso seja divulgada fora da **Hexágono Engenharia**.	Público geral	Informações publicadas dentro do site da **Hexágono Engenharia**, na internet, notícias, campanhas sociais.

É crucial ressaltar que todos os documentos produzidos ou manipulados dentro da **Hexágono Engenharia** devem ser devidamente classificados de acordo com as diretrizes estabelecidas neste documento. Além disso, é imprescindível que cada documento contenha as tarjas de identificação correspondentes à sua classificação.
Ademais, todos os colaboradores têm a responsabilidade de estar vigilantes em relação ao phishing e relatar imediatamente qualquer atividade suspeita. A detecção precoce e a notificação rápida são fundamentais para mitigar os riscos associados a esse tipo de ameaça.

Nesse sentido, em caso de detecção de quaisquer incidentes de segurança da informação, é fundamental que a pessoa envolvida comunique imediatamente ao setor de TI, por meio da abertura de um chamado. Os responsáveis pelo setor serão responsáveis pelo preenchimento do relatório de segurança e privacidade de dados dentro da organização junto ao Comitê de Governança de Dados. Essa análise será feita com objetivo de avaliar o incidente, seus impactos e as medidas necessárias a serem tomadas.

6.2 Diretrizes Específicas

I. E-mail

O e-mail corporativo da **Hexágono Engenharia** destina-se exclusivamente a fins corporativos e relacionados às atividades do colaborador dentro da instituição. A utilização deste serviço para fins pessoais não é permitida, bem como não é permitido nenhuma ação que possa prejudicar a **Hexágono Engenharia** ou impactar o tráfego da rede.

Por exemplo, enviar propagandas para uma grande quantidade de contatos utilizando o e-mail corporativo pode sobrecarregar a rede e prejudicar a comunicação interna. Existem ferramentas específicas para esse fim, e o uso do e-mail corporativo para tal atividade é proibido.

Incluímos abaixo as condutas proibidas aos colaboradores no uso do correio eletrônico da **Hexágono Engenharia:**

a. Enviar mensagens não solicitadas para múltiplos destinatários, a menos que relacionadas a atividades legítimas da empresa;

b. Utilizar o endereço de e-mail do departamento ou o nome de usuário de outra pessoa sem autorização;

c. Enviar mensagens que possam expor o remetente e/ou a **Hexágono Engenharia** a ações civis ou criminais;

d. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal do proprietário;

e. Falsificar informações de endereçamento ou adulterar cabeçalhos para ocultar a identidade do remetente e/ou destinatário, com o intuito de evitar sanções;

f. Apagar mensagens de e-mail relevantes

g. Produzir, transmitir ou divulgar mensagens que conflitem ou contrariem os interesses da **Hexágono Engenharia**; contenham ameaças eletrônicas, como spam, mail bombing e vírus de computador; incluam arquivos com código executável ou extensões que representem risco à segurança, busquem acesso não autorizado a computadores, servidores ou redes, tenham como objetivo interromper serviços, servidores ou redes de computadores de forma ilícita ou não autorizada, tencionem burlar sistemas de segurança, visem secretamente vigiar ou assediar outros usuários; acessem informações confidenciais sem autorização explícita; acessem informações que possam causar prejuízos; incluam imagens criptografadas ou mascaradas; contenham conteúdo considerado impróprio, obsceno ou ilegal; tenham caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador ou pornográfico, entre outros; contenham perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental, ou outras situações protegidas; tenham fins políticos locais ou nacionais (propaganda política); incluam

material protegido por direitos autorais sem a permissão do detentor dos direitos.

II. Internet

As atuais diretrizes da **Hexágono Engenharia** visam primordialmente promover um comportamento essencialmente ético e profissional no uso da internet. Embora a conexão direta e constante da rede corporativa da instituição com a internet ofereça um vasto potencial de benefícios, também abre portas para riscos significativos aos ativos de informação.

Toda informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, em total conformidade legal, **a Hexágono Engenharia** reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando garantir o cumprimento de sua Política de Segurança da Informação.

Ao monitorar a rede interna, a **Hexágono Engenharia** pretende garantir a integridade dos dados e programas. Qualquer tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem devido credenciamento e autorização, será considerada inadequada, e os riscos associados serão comunicados ao colaborador e ao respectivo gestor.

O uso de qualquer recurso para atividades ilícitas acarretará ações administrativas e penalidades decorrentes de processos civil e criminal, com a instituição cooperando ativamente com as autoridades competentes.

Apenas colaboradores autorizados, por seus gestores, podem copiar, capturar, imprimir ou enviar imagens da tela para terceiros, seguindo normas internas de uso de imagens, Leis de Direitos Autorais, Lei Geral de Proteção de Dados, proteção de imagem garantida pela Constituição Federal e demais dispositivos legais.

É vedada a divulgação e/ou compartilhamento indevido de informações administrativas em listas de discussão, sites ou comunidades online, salas de chat, comunicadores instantâneos ou qualquer outra tecnologia correlata na internet.

Colaboradores com acesso à internet podem fazer download apenas de programas relacionados às suas atividades na **Hexágono Engenharia** e devem regularizar a licença e o registro desses programas, com autorização da equipe de TI, por meio de abertura de chamado.

O uso não autorizado de softwares com direitos autorais, marcas registradas ou patentes é expressamente proibido. Qualquer software não autorizado será removido pela equipe de TI.

É estritamente proibido aos colaboradores utilizar recursos da **Hexágono Engenharia** para download ou distribuição de software ou dados pirateados, atividade considerada ilegal conforme a legislação nacional.

O acesso a softwares peer-to-peer (como Kazaa, BitTorrent, entre outros) não é permitido, assim como o acesso a sites de proxy.

III. Senhas e dispositivos de identificação

Os dispositivos de identificação e senhas têm como objetivo resguardar a identidade dos colaboradores da **Hexágono Engenharia**, impedindo que terceiros se façam passar por eles perante a instituição e/ou outros.

É importante lembrar ainda que uso indevido dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime conforme o Código Penal Brasileiro (art. 307 – falsa identidade).

Todos os dispositivos de identificação utilizados na **Hexágono Engenharia**, como número de registro do colaborador, crachá, identificações de acesso aos sistemas, certificados e assinaturas digitais, e dados biométricos devem estar vinculados de forma inequívoca aos documentos oficiais reconhecidos pela legislação brasileira.

O usuário associado a esses dispositivos de identificação é responsável por seu uso adequado perante a instituição e a legislação (cível e criminal). Não é permitido

compartilhar dispositivos de identificação pessoal com terceiros sob nenhuma circunstância.

Se houver um login compartilhado por mais de um colaborador, a responsabilidade perante a **Hexágono Engenharia** e a legislação (cível e criminal) recairá sobre os usuários que o utilizarem. Somente serão responsabilizados os usuários se houver conhecimento ou solicitação do gestor para uso compartilhado.

O Departamento de Recursos Humanos da **Hexágono Engenharia** é responsável pela emissão e controle dos documentos físicos de identidade dos colaboradores, enquanto o departamento de TI é responsável pela criação da identidade lógica dos colaboradores na instituição.

Os visitantes, estagiários, colaboradores e prestadores de serviços, sejam pessoas físicas ou jurídicas, devem ser devidamente identificados. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deve trocar imediatamente sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador devem utilizar senhas com tamanho variável, contendo no mínimo 12 caracteres alfanuméricos, incluindo caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).

Já os usuários com perfil de administrador ou acesso privilegiado devem utilizar senhas com no mínimo 15 caracteres alfanuméricos, incluindo caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).

Cada usuário é responsável por memorizar sua própria senha, bem como proteger e guardar os dispositivos de identificação designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos não criptografados (Word, Excel, etc.). Elas também não devem ser baseadas em informações pessoais, como nome próprio, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento, e não devem ser combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Após 5 (cinco) tentativas de acesso malsucedidas, a conta do usuário será bloqueada. Para desbloquear, o usuário deve entrar em contato com o departamento de TI da **Hexágono Engenharia** e confirmar sua identidade.

Os usuários podem alterar sua própria senha e devem ser orientados a fazê-lo caso suspeitem que terceiros tenham acesso indevido ao seu login/senha. As senhas devem ser alteradas no máximo a cada 90 (noventa) dias. Sistemas críticos e sensíveis para a instituição e logins com privilégios administrativos devem exigir a troca de senhas a cada 90 (noventa) dias, com sistemas que forcem a troca dentro deste prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, ao ocorrer demissão, pedido de demissão, término de contrato ou serviço, férias, afastamentos ou outras situações similares, o Departamento de Recursos Humanos deve comunicar imediatamente o Departamento de Tecnologia da Informação para tomar as devidas providências. Caso o colaborador esqueça sua senha, ele deve formalmente solicitar sua troca.

IV. Computadores e Recursos Tecnológicos

Os equipamentos disponibilizados aos colaboradores são de propriedade da **Hexágono Engenharia** e devem ser utilizados e manipulados de maneira apropriada para atividades relacionadas aos interesses da instituição, seguindo as orientações contidas nessa Política de Segurança da Informação.

Qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação nos equipamentos deve ser realizado somente com o conhecimento prévio e a supervisão de um técnico do departamento de TI da **Hexágono Engenharia.**

As atualizações e correções de segurança do sistema operacional ou aplicativos só podem ser realizadas após validação no ambiente de homologação e disponibilização pelo fabricante ou fornecedor.

Todos os sistemas e computadores devem ter software antivírus instalado, ativado e atualizado regularmente. Em caso de suspeita de vírus ou problemas de

funcionamento, o usuário deve contatar o departamento técnico responsável por meio do registro de chamado.

A transferência e/ou divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), só pode ser feita mediante identificação do solicitante, verificação positiva e necessidade real do destinatário bem como deve haver a aprovação do gestor e do setor de TI.

Arquivos pessoais e/ou não relacionados ao negócio da **Hexágono Engenharia** (como fotos, músicas, vídeos etc.) não devem ser copiados/movidos para os drives de rede, a fim de evitar sobrecarga no armazenamento nos servidores. Caso tais arquivos sejam identificados, podem ser excluídos definitivamente mediante comunicação prévia ao usuário, sem prejuízo da aplicação das medidas disciplinares cabíveis

Documentos essenciais para as atividades dos colaboradores devem ser salvos nos drives de rede. Arquivos gravados apenas localmente nos computadores (por exemplo, no drive C:) não são respaldados e podem ser perdidos em caso de falha no computador, sendo de responsabilidade do usuário.

Os colaboradores e detentores de contas privilegiadas não devem executar nenhum comando ou programa que sobrecarregue os serviços na rede corporativa sem prévia solicitação e autorização do departamento de TI.

No uso dos computadores, equipamentos e recursos de informática devem também seguir as seguintes regras:

a. Computadores de uso individual (no caso de terceiros e parceiros da Hexágono) devem ter senha de BIOS para restringir o acesso não autorizado, definidas pelo departamento de TI, que mantém acesso para manutenção dos equipamentos.

b. Os colaboradores devem reportar ao departamento técnico qualquer dispositivo estranho conectado ao seu computador.

c. Não é permitido abrir ou manipular computadores ou equipamentos de informática para reparos, a menos que seja realizado por um técnico do departamento de TI da **Hexágono Engenharia** ou por terceiros contratados.

d. Todos os modems internos ou externos devem ser removidos ou desativados para evitar invasão de informações, programas ou vírus, exceto em casos especiais autorizados.

e. É expressamente proibido consumir alimentos, bebidas ou fumar na mesa de trabalho e próximo aos equipamentos.

f. Os equipamentos devem ser configurados conforme os controles de segurança exigidos pela Política de Segurança da Informação e pelas normas da instituição, com os terminais de computador e impressoras bloqueados quando não estiverem em uso, conforme previsto pela Norma de Autenticação.

g. Todas as senhas padrões dos recursos tecnológicos devem ser alteradas imediatamente após a aquisição do recurso.

Adicionalmente, não é permitido pela **Hexágono Engenharia** tentar ou obter acesso não autorizado a outros computadores, servidores ou redes; burlar sistemas de segurança; acessar informações confidenciais sem autorização; realizar atividades ilegais, como hospedar pornografia ou utilizar software pirata.

V. Dispositivos móveis

A **Hexágono Engenharia** visa promover a facilidade de mobilidade e o fluxo de informações entre seus colaboradores, permitindo o uso de equipamentos portáteis. Entende-se por "dispositivo móvel" qualquer equipamento eletrônico com capacidade de mobilidade de propriedade da empresa ou aprovado e autorizado pelo departamento de TI, incluindo notebooks, smartphones, pendrives e tablets.

Como proprietária dos dispositivos fornecidos, a **Hexágono Engenharia** reserva-se o direito de inspecioná-los a qualquer momento, caso seja necessário realizar manutenção de segurança.

É responsabilidade de cada colaborador realizar backups regulares dos dados de seu dispositivo móvel, mantendo-os separados do próprio dispositivo. O suporte técnico aos dispositivos móveis da empresa e aos seus usuários seguirá os mesmos procedimentos dos equipamentos da organização.

Todos os colaboradores devem utilizar senhas de bloqueio automático em seus dispositivos móveis. Não é permitida a alteração da configuração dos sistemas operacionais dos dispositivos sem comunicação e autorização prévias da área responsável e sem a presença de um técnico de TI.

O uso de programas e aplicativos não autorizados ou não instalados por um técnico de TI é proibido. A reprodução não autorizada de softwares instalados nos dispositivos móveis da empresa constitui infração aos direitos autorais do fabricante.

O uso da rede banda larga em locais conhecidos pelo colaborador, como sua casa, hotéis, fornecedores e clientes, é permitido. Em caso de furto ou roubo de um dispositivo móvel da empresa, o colaborador deve notificar imediatamente seu gestor e o departamento de TI, além de registrar um boletim de ocorrência junto às autoridades policiais.

O colaborador assume total responsabilidade por quaisquer danos causados à **Hexágono Engenharia** e/ou a terceiros devido ao uso indevido do dispositivo móvel.

Colaboradores que desejem utilizar equipamentos portáteis particulares ou acessórios conectados à rede da empresa devem obter autorização prévia do departamento de TI. Equipamentos não fornecidos pela instituição não serão validados para uso e conexão na rede corporativa.

VI. Datacenter

No Datacenter da **Hexágono Engenharia**, as seguintes diretrizes são seguidas para garantir a segurança e o bom funcionamento:

a) Acesso Restrito e Controle de Chaves: O acesso ao Datacenter é restrito por fechadura, com a chave sob responsabilidade da recepção, garantindo controle sobre quem entra no ambiente.

b) Cadastro de Acesso para Colaboradores: Em locais sem colaboradores da área de tecnologia da informação, pessoas de outros departamentos podem ser cadastradas no sistema de acesso para realizar atividades operacionais, como troca de fitas de backup e suporte a problemas técnicos.

c) Limpeza e Organização: O Datacenter deve ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira só pode ser realizado com a colaboração do Departamento de Serviços Gerais.

d) Proibição de Alimentos e Bebidas: Não é permitida a entrada de alimentos, bebidas, produtos fumígenos ou inflamáveis no Datacenter, garantindo a segurança dos equipamentos e da infraestrutura.

e) Controle de Equipamentos: A entrada ou retirada de quaisquer equipamentos do Datacenter só pode ocorrer com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal do responsável pelo Datacenter, conforme os termos do Procedimento de Controle e Transferência de Equipamentos.

VII. Backup

O backup é uma parte crucial da estratégia de segurança da informação da **Hexágono Engenharia**. Para garantir sua eficácia, seguimos algumas diretrizes:

a) Agendamento Automatizado: Todos os backups são automatizados por sistemas de agendamento automatizado, executados preferencialmente fora do horário comercial, durante as chamadas "janelas de backup", quando não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

b) Atualização e Monitoramento: Os colaboradores responsáveis pela gestão dos sistemas de backup realizam pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida do software, sugestões de melhorias, entre outros.

c) Identificação e Organização das Mídias: As fitas de backup são devidamente identificadas, preferencialmente com etiquetas não manuscritas, garantindo uma organização profissional. Alterações de nome são registradas para manter o controle sobre as mídias.

d) Monitoramento do Tempo de Vida das Mídias: O tempo de vida e uso das mídias de backup são monitorados e controlados pelos responsáveis. Mídias que apresentam erros são formatadas e testadas. Caso o erro persista, são inutilizadas.

e) Limpeza das Unidades de Backup: O dispositivo de limpeza é inserido periodicamente nas unidades de backup, conforme o Procedimento de Controle de Mídias de Backup.

f) Regra de Retenção Especial: Backups críticos para o bom funcionamento dos negócios da empresa seguem uma regra de retenção especial, de acordo com os procedimentos específicos e a Norma de Classificação da Informação, seguindo as determinações fiscais e legais.

g) Restauração Após Erros: Em caso de erro de backup e/ou restore, o procedimento é realizado assim que o problema é identificado e solucionado, no primeiro horário disponível.

h) Testes de Restauração: Testes de restauração (restore) de backup são executados periodicamente, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup. Durante esses testes, os arquivos são restaurados em um local diferente do original para evitar a sobreposição de arquivos válidos.

VIII. Antivírus

A **Hexágono Engenharia** exige a utilização de softwares de segurança contra vírus e outros programas maliciosos em todos os seus computadores e servidores. Esses softwares são selecionados pela equipe de TI após uma cuidadosa avaliação. Além

disso, a atualização automática desses é configurada no próprio software e é realizada diariamente.

IX. Controle de acessos

Como parte das medidas de segurança da informação da **Hexágono Engenharia**, foi implantado um rigoroso controle de acessos, que inclui o mapeamento detalhado de todos os usuários, softwares e aplicativos da empresa, bem como uma revisão dos usuários autorizados a acessar as pastas da rede corporativa. Essa abordagem proporciona uma visibilidade completa sobre quem tem acesso aos recursos de informação da empresa, assegurando que apenas usuários autorizados possam interagir com os sistemas e dados sensíveis.

7.0 MONITORAMENTO E ACOMPANHAMENTO

7.1 Acompanhamento das ações

Anualmente, o Comitê de Governança de Dados, em colaboração com o setor de TI, conduzirá um acompanhamento das ações relacionadas à segurança da informação, podendo promover auditorias internas com este foco específico. Este processo englobará a coleta e análise dos treinamentos e iniciativas realizadas, revisão dos termos e contratos firmados, bem como a supervisão dos riscos identificados e dos incidentes de segurança da informação registrados, juntamente com os controles implementados.

Adicionalmente, o Comitê monitorará todas as ações envolvendo terceiros, fornecedores e prestadores de serviços que venham ao seu conhecimento, assegurando a aplicação da Política de Segurança da Informação a todos os públicos pertinentes.

8.0 OUVIDORIA

A **Hexágono Engenharia** também oferece um canal de ouvidoria como meio anonimizado para o recebimento de relatos de incidentes de segurança da informação.

Trata-se de uma ferramenta tecnológica terceirizada que permite que colaboradores e partes interessadas comuniquem suspeitas de violações à Política de Segurança da Informação, ao Código de Conduta, ao Manual do Colaborador, assim como a outras políticas, procedimentos e normas internas ou à legislação aplicável. Além disso, trata-se de um recurso essencial para detectar, sanar e remediar possíveis violações aos valores da empresa.

9.0 VIOLAÇÕES À POLÍTICA

Aplicações equivocadas, desproporcionais ou a completa falta de gestão de consequências para os públicos que se relacionam com a **Hexágono Engenharia** podem ser relatadas por meio da Ouvidoria da empresa. Além disso, é responsabilidade dos gestores reportar situações envolvendo colaboradores e terceiros ao Comitê de Governança de Dados, às Gerências e à Diretoria, nos casos apropriados para a aplicação da Política de Gestão da Consequência(POL-COM-XXX).

10.0 DISPOSIÇÕES FINAIS E RESULTADOS ESPERADOS

10.1 Disposições finais

Esta política sempre que necessário deverá ser revisada pelo Comitê de Governança de Dados, o qual deve identificar ativamente os pontos de aprimoramento observados durante o período anterior, de forma a promover a melhoria contínua do documento e do processo decisório da **Hexágono Engenharia.**

10.2 Resultados esperados

A implementação efetiva desta Política Segurança da Informação na **Hexágono Engenharia** visa atingir os seguintes resultados:

Proteção dos Ativos de Informação: A aplicação consistente das diretrizes da PSI garantirá a proteção adequada dos ativos de informação da empresa, incluindo dados confidenciais, sistemas e redes, contra ameaças internas e externas.

Conformidade Legal e Regulatória: A PSI assegurará que a **Hexágono Engenharia** esteja em conformidade com todas as leis, regulamentos e normas aplicáveis relacionadas à segurança da informação, evitando potenciais violações e sanções legais.

Prevenção de Incidentes de Segurança: A adoção das medidas preventivas recomendadas na PSI ajudará a reduzir a probabilidade de ocorrência de incidentes de segurança, tais como violações de dados, ataques cibernéticos e interrupções no sistema.

Cultura de Conscientização em Segurança: A política promoverá uma cultura organizacional de conscientização em segurança da informação, incentivando os colaboradores a compreenderem a importância da proteção dos dados e a adotarem práticas seguras em seu dia a dia.

Resposta Eficiente a Incidentes: A PSI estabelecerá procedimentos claros e eficientes para a gestão de incidentes de segurança, garantindo uma resposta rápida e coordenada em caso de violações de segurança ou emergências cibernéticas.

Fortalecimento da Confiança dos Stakeholders: Ao demonstrar um compromisso claro com a segurança da informação, a **Hexágono Engenharia** fortalecerá a confiança de seus clientes, parceiros de negócios e demais stakeholders na proteção de seus dados e informações.

Redução de Riscos e Custos: A implementação eficaz da PSI ajudará a reduzir os riscos de incidentes de segurança e os custos associados a violações de dados, como multas regulatórias, perda de reputação e interrupções operacionais.

Sustentabilidade do negócio: A integridade e a conformidade com os as políticas e procedimentos contribuirão para a sustentabilidade a longo prazo do negócio, fortalecendo a continuidade das operações e a reputação da empresa no mercado.

11.0 CONTROLE DE REVISÃO

Nº REVISÃO	DATA	MOTIVO DA REVISÃO
00	30/04/2024	EMISSÃO INICIAL.

12.0 ANEXOS

PRO-COM-001 - Procedimento de Gestão de Incidentes de Segurança da Informação

FO-GEP-019- Termo de Sigilo e Confidencialidade.

FO-SGI-022 - Termo de Responsabilidade pela Guarda e Uso do Equipamento

13.0 REFERÊNCIAS

ABNT, NBR ISO/IEC 27001 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

ABNT, NBR ISO/IEC 27002 Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

ANPD. SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE. 2021

ANPD: CHECKLIST DE MEDIDAS DE SEGURANÇA PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE. 2021

BRASIL: Regulamento de Comunicação de Incidente de Segurança, Resolução CD/ANPD nº 15 de abril de 2024, ANPD.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL. Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet

FONTES, Edison. Políticas e Normas para a Segurança da Informação. 1. ed. Rio de Janeiro, 2012.

HINTZBERGEN, J. HINTZBERGEN, K. SMULDERS, A. et al. Fundamentos de Segurança da Informação. 1. ed. Rio de Janeiro, 2018.