CONTROLE DE APROVAÇÃO

ELABORADO	REVISADO PELO ÓRGÃO NORMATIVO	APROVADO
Elilton Ferreira	Esther Menezes	Elilton Ferreira

HISTÓRICO DA ÚLTIMA MODIFICAÇÃO

EDIÇÃO	DATA	ALTERAÇÕES EM RELAÇÃO À REVISÃO ANTERIOR
1ª	15/12/2023	Inclusão do termo Privacidade nos Itens 3, 4.1 e 4.2.1

ÍNDICE

1. OBJETIVO

Esta Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da NÉOS para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários, deve, portanto, ser cumprida e aplicada em todas as áreas da NÉOS.

O objetivo desta Política é estabelecer as diretrizes, princípios e as regras básicas do Sistema de Gestão da Segurança da Informação (SGSI) na entidade.

Os usuários deste documento são todos os empregados da NÉOS, assim como as partes externas relevantes.

2. RESPONSABILIDADES

O principal responsável pela Segurança da Informação da NÉOS é o Gerente de Tecnologia e Inovação. Tendo como principais atribuições:

a) Garantir a implementação e operação do SGSI de acordo com os requisitos da norma ABNT ISO/IEC 27001;

b) Reportar sobre o desempenho do SGSI para a Direção da NÉOS;

c) Implementar programas de conscientização e treinamentos de segurança da informação para todos os colaboradores da NÉOS;

d) Tratar todos os incidentes de segurança da informação de acordo com sua criticidade;

e) Elaborar políticas e procedimentos referentes a segurança da informação para garantir o alcance dos objetivos de segurança;

Compete a TODOS os colaboradores da NÉOS:

a) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

b) Cumprir esta política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

c) Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio;

d) Comunicar todos os incidentes e as fragilidades de segurança da informação que forem identificadas conforme estabelecido no procedimento de Gestão de Incidentes.

Será de inteira responsabilidade de cada empregado, todo prejuízo ou dano que vier a sofrer ou causar à NÉOS e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Cabe às gerências, além das atribuições de seus cargos, as seguintes atividades:

a) Garantir o cumprimento desta política de segurança, por parte de seus empregados;

b) Identificar e tratar os riscos relacionados às atividades das suas respectivas áreas;

c) Identificar os desvios praticados e adotar as medidas corretivas apropriadas;

d) Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os empregados sob a sua gestão;

e) Atribuir aos empregados, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação da NÉOS;

f) Solicitar dos empregados a assinatura da Declaração de Aceitação da documentação do SGSI, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da NÉOS;

g) Antes de conceder acesso às informações da NÉOS, exigir a assinatura do Acordo de Confidencialidade dos empregados e prestadores de serviços que não estejam cobertos por um contrato existente;

h) Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta Política.

Outras responsabilidades específicas poderão ser definidas nas demais políticas e procedimentos de Segurança da Informação.

3. CONCEITUAÇÃO

Para as finalidades previstas neste documento, considera-se:

Ativos de Informação - os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações

em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Confidencialidade – características das informações que não podem ser divulgadas e disponibilizadas para pessoas não autorizadas.

Disponibilidade - características das informações acessíveis e utilizáveis somente por pessoas autorizadas.

Integridade - características das informações que não podem ser modificadas, suprimidas ou destruídas de maneira não autorizada ou acidental;

Privacidade - direito de controlar o acesso e uso de suas informações pessoais, assegurando que sejam resguardadas contra acesso e divulgação não autorizados.

Incidente de Segurança da Informação - evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo.

Prestadores de Serviço - todas as pessoas que prestam serviços a entidade que não pertencem ao quadro funcional da empresa. São considerados prestadores de serviços: terceiros, consultores, auditores entre outros.

Segurança da informação – meio de preservação da confidencialidade, integridade e disponibilidade da informação;

Sistema de Gestão da Segurança da Informação - a parte do Sistema de Gestão que cuida do planejamento, implementação, manutenção, revisão e aprimoramento da segurança da informação.

Usuários - as pessoas que utilizam os sistemas de informação (empregados, prestadores de serviços e estagiários).

4. DISPOSIÇÕES GERAIS

4.1 Diretrizes Gerais

A informação utilizada na NÉOS deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua confidencialidade, integridade, disponibilidade, autenticidade e privacidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

A Segurança da Informação na NÉOS estabelece os principais controles, denominados diretrizes:

a) As informações da NÉOS e dos seus participantes em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;

b) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;

c) A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da NÉOS em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;

d) Sempre que possível, todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um empregado ou equipe de empregados, para que a atividade não seja executada e controlada por uma única pessoa;

e) O acesso às informações e recursos só deve ser feito se devidamente autorizado;

f) A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

g) A identificação de qualquer empregado deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas. A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;

h) Os riscos às informações da NÉOS devem ser reportados à área de TI.

4.2 Gestão da Segurança da Informação

4.2.1. Objetivos e Medição

Os objetivos gerais para a gestão de segurança da informação são:

- Proteger as informações do negócio da NÉOS e as informações dos participantes que estejam sob nossa custódia (guarda) preservando sua confidencialidade, integridade, disponibilidade e privacidade;

- Encorajar a gestão e equipe a manter um nível apropriado de conscientização, conhecimento e habilidades de forma a minimizar a ocorrência e a gravidade dos incidentes de segurança da informação;

- Garantir que a organização possa continuar suas atividades no caso de incidentes significativos de segurança da informação;

Os objetivos acima estão alinhados com os objetivos de negócios e a estratégia da organização.

O responsável pelo SGSI é responsável por propor novos objetivos de segurança da informação que deverão ser aprovados pela Diretoria Executiva anualmente.

A NÉOS irá mensurar o atendimento de todos os objetivos. O responsável pelo SGSI é responsável por definir o método para a medição da realização dos objetivos. Recomenda-se que a medição seja executada a cada seis meses e a análise e avaliação dos resultados da medição será reportada para a alta direção como entrada para a reunião análise crítica.

4.2.2. Requisitos de Segurança da Informação

Esta Política e todo o SGSI deve estar em conformidade com os requisitos legais e regulamentares relevantes à organização na área de segurança da informação, bem como com as obrigações contratuais.

4.2.3 Controles da Segurança da Informação

Os processos para selecionar os controles estão definidos na Metodologia de Avaliação e Tratamento de Riscos descritas no Manual de Gestão da Qualidade.

4.2.4. Continuidade de Negócios

A gestão de continuidade de negócios é descrita no Plano de Continuidade de Negócios e no Plano de Recuperação de Desastres.

4.2.5. Comunicação da Política de Segurança da Informação

O responsável pelo SGSI deve garantir que todos os empregados da NÉOS, bem como as partes interessadas relevantes conheçam esta Política. A comunicação desta Política será:

- Colaboradores: A PSI está disponível na rede interna com acesso irrestrito e é divulgada regularmente para todos os empregados/estagiários de acordo com o Plano de Comunicação.
- Demais partes interessadas: Uma versão apropriada da PSI estará disponível no site da NÉOS acessível através do endereço: https://neosprevidencia.com.br/

4.2.6. Proteção e Privacidade de Dados Pessoais

Todas as áreas, empregados, bem como todas as partes interessadas pertinentes, que, pela natureza de sua atividade, acessem dados pessoais, devem zelar pelo cumprimento dos requisitos estabelecidos na legislação de proteção de dados pessoais e na Política de Privacidade e Proteção de Dados da NÉOS.

4.2.7. Sanções

As violações de segurança devem ser informadas ao responsável pelo SGSI, por meio de e-mail, telefone ou registro no sistema interno. Toda violação ou desvio será investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Vazamento de dados pessoais.

O descumprimento de quaisquer itens desta política e das normas derivadas dela implicará, conforme a gravidade, nas sanções abaixo descritas e na legislação vigente:

a) Enquadramento no Código de Ética;
b) Advertência;
c) Suspensão;
d) Demissão.

5. APROVAÇÃO

Este documento foi aprovado no dia 24 de setembro de 2020. O proprietário do documento é o Gerente de Tecnologia e Inovação, que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

6. CONTROLE DE REGISTROS

Todos os registros devem ser:

- Manuseados com cuidado, para evitar danos, deterioração ou perda;
- Arquivados e mantidos de forma adequada, a fim de garantir a integridade de suas informações.

Código	Identificação	Origem	Armazenamento (área)	Proteção (suporte)	Recuperação		Tipo de Arquivo		Tempo de Retenção	Disposição
					Indexação	Acesso	Ele.	Fis.		
	Objetivos	ACC.GS. N01	Nuvem	Backup	H:	Irrestrito	X		2 anos	Deletar
	Análise crítica	ACC.GS. N01	Nuvem	Backup	H:	Irrestrito	X		2 anos	Deletar

7. REFERÊNCIAS BIBLIOGRÁFICAS

Norma ISO/IEC 27001, cláusulas 5.2 e 5.3

Norma ISO/IEC 27002 - Código de Prática para a Gestão de Segurança da Informação.

Código de Ética e Conduta da NÉOS

Guia PREVIC - Melhores Práticas em Governança – 2012

Resolução CGPC nº 13/2004 – Princípios, regras e práticas de governança, gestão e controles internos a serem observados pelas entidades fechadas de previdência complementar - EFPC

Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD)