PENTÁGONO

www.pentagonotrustee.com.br

Rio de Janeiro
Centro Empresarial de Barrashopping
Av. das Américas 4.200, 302/303/304
Bloco 08 - Ala B Barra da Tijuca
22640-102

São Paulo
Edifício Hyde Park
Av. Faria Lima 2.954, conj. 101 Itaim Bibi
01451-000

POLÍTICA DE CIBERSEGURANÇA – DIVULGAÇÃO AO PÚBLICO

(v.2 nov/21)

OBJETIVO: Dar ciência ao público em geral das diretrizes de Cibersegurança, as quais visam proteger os ativos de tecnologia e dados da **PENTÁGONO S.A. DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS** ("**PENTÁGONO**"), bem como informar às áreas cabíveis e atribuir as responsabilidades para cumprimento da Política de Cibersegurança.

I. DAS DISPOSIÇÕES GERAIS

I.A) Abrangência

A Política de Cibersegurança da PENTÁGONO destina-se a todos os colaboradores, parceiros, fornecedores, prestadores de serviços e clientes da PENTÁGONO.

Para os fins do disposto na Política de Cibersegurança, o termo "Colaboradores" abrange todos os empregados, estagiários e administradores da PENTÁGONO.

Toda a atividade da PENTÁGONO deve respeitar os princípios estabelecidos na Política de Cibersegurança; e tais princípios devem ser aplicados a todos os que estão acima mencionados.

I.B) Diretrizes

A PENTÁGONO tem como objetivo atingir um alto padrão de Cibersegurança. Por isso, é comprometida com a confidencialidade, integridade e disponibilidade de todos os ativos físicos e lógicos de informação da empresa, garantindo que os requisitos legais, operacionais e contratuais sejam cumpridos. A preocupação com os riscos cibernéticos é comum aos diversos níveis de gestão e deve ser um compromisso individual de todos os Colaboradores.

I.C) Aspectos Gerais

O presente visa estabelecer princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, garantindo a proteção adequada dos ativos e dos dados, garantindo assim a identificação, proteção, detecção, resposta e recuperação de eventos em casos de eventual incidente de segurança na PENTÁGONO.

I.C.i) Identificação

Desenvolver uma cultura organizacional para gerenciar o risco de Cibersegurança, sistemas, pessoas, ativos, dados e capacidades. Além disto, visa realizar o registro, análise de causa e impacto, e controle dos efeitos de incidentes, incluindo informações recebidas de terceiros, utilizando como base os seguintes processos e recursos, a fim de mitigar riscos:

i. Regulamentações Vigentes;
ii. Diretrizes e normas do Banco Central do Brasil;
iii. Gerenciamento de Ativos;
iv. Ambiente de Negócios;
v. Governança;
vi. Avaliação de Risco;
vii. Estratégia de Gerenciamento de Riscos.

I.C.ii) Proteção

Desenvolver e implementar salvaguardas apropriadas para garantir o controle e a mitigação de riscos, incluindo, mas não se limitando a realização de:

i. Controle de acesso;
ii. Conscientização e treinamentos;
iii. Processos e procedimentos para proteção das informações.

I.C.iii) Detecção

Desenvolver e implementar ações estruturadas para identificar a ocorrência de eventuais eventos que causem riscos e comprometam a Cibersegurança, incluindo, mas não se limitando a:

i. Monitoramento de eventos e anomalias;
ii. Monitoramento contínuo de segurança, incluindo parceiros, fornecedores, prestadores de serviços e clientes;
iii. Processo de detecção, análise e mitigação de riscos;
iv. Plano de resposta a incidentes;
v. Comunicação;
vi. Monitoramento e melhoria contínua.

I.C.iv) Recuperação

Desenvolver e programar ações sustentáveis para manter os planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um eventual incidente de Cibersegurança, incluindo, mas não se limitando a:

i. Comunicação junto aos envolvidos;
ii. Mapeamento e implementação de melhorias;
iii. Plano de recuperação.

II. DAS RESPONSABILIDADES

II.A) Colaboradores, Parceiros, Fornecedores, Prestadores de Serviços e Clientes

i. Salvaguardar todo recurso e informação da PENTÁGONO criado ou utilizada nas suas atividades, inclusive, mas não se limitando a distribuição não autorizada, acesso indevido, modificação ou destruição;
ii. Conhecer suas responsabilidades a respeito da Cibersegurança, atuando de forma segura, ética e legal na utilização dos recursos e dados, primando pela preservação da integridade, confidencialidade e disponibilidade das informações da empresa;
iii. Relatar ao TI através do e-mail ti@pentagonotrustee.com.br qualquer situação que represente desvio ou violação desta Política bem como das normas vigentes.

III. DA CONTRATAÇÃO DE SERVIÇOS EM NUVEM *(cloud computing)*

Previamente à contratação de serviços relevantes de processamento e armazenamento de informações em nuvem *(cloud computing)*, deverá ser verificado o cumprimento das exigências mínimas previstas no artigo 12 da Resolução CMN nº 4.893/21 ou da Resolução BCB nº 85/21 ou em qualquer outro normativo que venha a substituir os aqui mencionados.

IV. DAS INICIATIVAS PARA COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES DE CIBERSEGURANÇA

A PENTÁGONO permite que as empresas de informática por ela contratadas para prestação de serviços compartilhem entre si os incidentes eventualmente ocorridos, de forma a auxiliar na prevenção de incidentes de Cibersegurança, visto que os mesmos muitas vezes são similares.

Caso seja identificado qualquer incidente de Cibersegurança, será emitido o Relatório de Incidentes de Cibersegurança (Anexo I). O referido relatório será disponibilizado no site da PENTÁGONO.

V. DAS MEDIDAS DISCIPLINARES

As violações a esta Política estão sujeitas às ações disciplinares previstas nas normas internas e na legislação brasileira vigente.

LEGISLAÇÃO RELACIONADA

Resolução CMN nº 4.893, de 26 de fevereiro de 2021

Resolução BCB nª 85, de 08 de abril de 2021

Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018)

Anexo I – Modelo de Relatório de Incidentes de Cibersegurança

Relatório de Incidentes de Cibersegurança

A Pentágono S.A. Distribuidora de Títulos e Valores Mobiliários ("PENTÁGONO"), atendendo às exigências contidas na Resolução CMN nº 4.893/21 e conforme previsto na Política de Cibersegurança da PENTÁGONO, relata, por meio do presente, o abaixo identificado:

[•]

[•], [•] de [•] de [•].

_____

Diretor Responsável