HEMERA

Política de Segurança Cibernética

Sumário

Verificação e Atualização

✓ Esta política será atualizada a cada 12 (doze) meses, ou sempre que houver alterações, e tal atualização seguirá o mesmo fluxo de aprovação e divulgação.

✓ A área de *Compliance* é a responsável final por toda e qualquer alteração, atualização e divulgação.

Introdução

No mundo globalizado e digitalizado, a informação tornou-se um dos principais ativos à operação e atividades desenvolvidas por qualquer tipo de instituição. Tal como os ativos físicos e financeiros, a informação deve ser adequadamente manuseada e protegida contra ameaças internas ou externas. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças. É por isso que os reguladores e instituições privadas têm atuado constantemente para aperfeiçoar e monitorar os riscos ligados a segurança da informação e cibernética. Esta política formaliza o compromisso de nossa instituição em seguir os melhores padrões de segurança da informação e cibernética que emanam dos reguladores e autorreguladores.

Objetivo

O objetivo desta Política de Segurança Cibernética é definir processos e controles que a Hemera DTVM, doravante designada como “Hemera”, estabelece para proteção da informação e tratamento dos riscos e ameaças relacionadas à Segurança da Informação e Segurança Cibernética, com base na Resolução BCB nº 85, de 2021, o Guia Anbima de Cibersegurança e demais normas e disposições aplicáveis em seus códigos, principalmente o código de serviços qualificados e o código de administração de recursos de terceiros.

Esta política deve ser lida em conjunto com a política de segurança da informação, o manual de tecnologia da informação e a política de gestão de continuidade de negócios.

Abrangência

Aplica-se a todos os colaboradores, executivos, estagiários e prestadores de serviços - doravante designados em conjunto como colaboradores.

Definições/ Conceitos:

Segurança Cibernética: é a disciplina que concentra os esforços na proteção dos ativos de informação que estejam alocados em um ambiente virtual. O ambiente cibernético é uma resultante da interação de pessoas, softwares e serviços por meio de dispositivos tecnológicos e redes conectadas a estes dispositivos.

A crescente ameaça cibernética, somada à cada vez maior dependência dos sistemas digitais faz com que a segurança da informação e segurança cibernética **sejam uns dos principais riscos não financeiros para os negócios**. A proteção dos sistemas e da informação, de nossos negócios e de nossos clientes, constituem prioridade de primeiro nível, sendo um componente essencial dos objetivos corporativos da Hemera DTVM.

Principais ameaças cibernéticas:

1 – Ataques causados por Vírus:

- ✓ Spyware
- ✓ Ransomware
- ✓ Vírus ou malware; e
- ✓ Trojan Horse

2 – Ataques de DDOS - Negação de Serviços e acessos:

Em um ataque de DDoS (negação distribuída de serviço), um invasor sobrecarrega seu alvo com tráfego de Internet indesejado, indisponibilizando o destino pretendido. Um ataque de DDoS ao website, à aplicação da Web, às APIs, à rede ou à infraestrutura de data center de uma empresa pode causar tempo

de inatividade e impedir que usuários usem nossos serviços, obtenham informações ou realizem qualquer outro acesso. Durante estes ataques, os invasores usam muitas máquinas exploradas e dispositivos conectados pela Internet, smartphones, computadores pessoais e servidores de rede, para enviar uma inundação de tráfego para os alvos.

3 – Engenharia Social:

A engenharia social, no contexto de segurança da informação, refere-se à técnica pela qual uma pessoa procura persuadir outra, muitas vezes abusando da ingenuidade ou confiança do usuário, objetivando ludibriar, aplicar golpes ou obter informações sigilosas. As formas mais comuns de engenharia social são:

- ✓ Pharming;
- ✓ Vishing;
- ✓ Smishing;
- ✓ Phishing; e
- ✓ Acesso Pessoal.

Dentre as mais utilizadas, destacamos o uso de phishing. Técnica utilizada por cibercriminosos para enganar os usuários, através de envio de e-mails maliciosos afim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros. As abordagens dos e-mails de phishing podem ocorrem das seguintes maneiras:

- ✓ Quando procuram atrair as atenções dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade;
- ✓ Quando tentam se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de comércio eletrônico, entre outros sites populares;
- ✓ Quando tentam induzir os usuários a preencher formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;

Não é incomum os ataques de Phishing precederem alguns outros ataques.

- ✓ **Incidente de segurança cibernética:** todo e qualquer evento não esperado que gere algum tipo de instabilidade, quebra de política, violação da privacidade, da integridade, da confidencialidade e da disponibilidade dos dados da causando assim danos que prejudiquem nossos negócios, parceiros ou clientes;
- ✓ **Ataque cibernético:** é a exploração por parte de um agente malicioso para tirar proveito de ponto(s) fraco(s) com a intenção de alcançar um impacto negativo no alvo. Os atacantes podem ter como alvo os clientes, fornecedores e parceiros da Hemera, e podem gerar impactos substanciais para a continuidade de seus negócios.
- ✓ **Risco à segurança cibernética:** advêm de dentro e de fora da instituição. O impacto do risco à segurança cibernética engloba perda financeira, danos à reputação, multas regulatórias, perda de vantagem estratégica e interrupção de operações;
- ✓ **Ativos tecnológicos:** é qualquer dispositivo físico ou digital, equipamento ou outro componente do ambiente que suporte atividades relacionadas à informação; e
- ✓ **Threat intelligence:** consiste em todo conhecimento baseado em evidências, contexto, mecanismos e indicadores sobre ameaças existentes, correlacionando com os ativos tecnológicos que podem ser comprometidos a partir da exploração e concretização dessa ameaça.
- ✓ **Espaço cibernético:** engloba a internet, os sistemas de informação, os dispositivos móveis e as tecnologias digitais que dão suporte aos negócios, a infraestrutura e os serviços;

Objetivos da Segurança da Informação e Cibernética:

É a disciplina que concentra esforços contínuos à proteção dos ativos de informação, auxiliando a Organização a cumprir sua missão e valores. Para tanto, tem como objetivos:

- ✓ **Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
- ✓ **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais);
- ✓ **Disponibilidade:** garantir que as informações estejam disponíveis às pessoas autorizadas;
- ✓ **Privacidade:** garantir que todas as informações coletadas e armazenadas por nós para a prestação dos serviços previstos em contrato, por obrigação legal ou outras bases estabelecidas na Lei Geral de Proteção de Dados – LGPD 13.709/2018, permaneçam protegida, privadas e seguras contra ameaças externas ou por uso indevido.

Objetivos específicos da Segurança Cibernética:

A segurança cibernética pode ser resumida como a soma de práticas e controles de identificação, prevenção, proteção, detecção, resposta e recuperação frente as ameaças cibernéticas, a fim de proteger nossos ativos tecnológicos e garantir a confidencialidade, integridade, a privacidade e a disponibilidade das informações.

Responsabilidades pela segurança cibernética

Gestão de riscos e Compliance:

A área de compliance e gestão de riscos, junto a área de Infraestrutura de sistemas, é a responsável por garantir que a integridade, a confidencialidade, a privacidade e a disponibilidade das informações sejam mantidas frente a ataques cibernéticos. Sua missão reside na adoção de medidas técnicas e administrativas como:

- ✓ Elaboração de Políticas;
- ✓ Padronização de procedimentos e controles;
- ✓ Manutenção e realização de testes de aderência que demonstrem a eficácia dos controles implantados;
- ✓ Comunicação ao regulador em caso de incidentes cibernéticos;
- ✓ Governança e Gestão das Políticas de Segurança da Informação e Cibernética;

✓ Gestão de Acessos (Definição de Regras e Critérios) e Segregação de Funções;

✓ Atendimento das Auditorias;

✓ Adotar os mais elevados padrões de diligência na contratação de serviços de processamento, armazenamento ou computação em nuvem; e

✓ Disseminação da Cultura, Treinamento e Conscientização de Segurança da Informação e Cibernética, através de cursos ministrados internamente ou por terceiros contratados por nós para esta finalidade.

Infraestrutura de sistemas:

Cabe a infraestrutura de sistemas

- ✓ Entender, gerenciar e monitorar os riscos e controles ligados à segurança da informação e cibernética;
- ✓ Monitorar a saúde dos ativos de tecnologia;
- ✓ Gerenciar as senhas e logs dos principais sistemas utilizados pela instituição;
- ✓ Reportar e/ou escalar o risco de Segurança Cibernética (incluindo ativos relevantes, informações, sistemas e terceiros);
- ✓ Realizar testes de invasão sempre que necessário, visando detectar vulnerabilidades e avaliar a qualidade e suficiência dos controles dos ativos de TI; e
- ✓ Responder aos incidentes de segurança cibernética.

Funcionários, Prestadores de Serviços e Estagiários

Todo colaborador, prestador de serviço ou estagiário, deve observar e seguir as políticas, padrões e procedimentos estabelecidos pela instituição, sendo imprescindível sua compreensão do papel da Segurança da Informação e Segurança Cibernética no desenvolvimento e manutenção das atividades diárias. É de responsabilidade de cada colaborador, prestador de serviço ou estagiário, prejuízos ou

danos que vier a sofrer ou causar à Hemera ou a terceiros, em decorrência da não obediência às políticas aqui referidas.

Controles Específicos de Segurança da Informação e Cibernética:

- ✓ Gerenciador de logs;
- ✓ Trilhas de auditoria;
- ✓ Diligência de fornecedores e parceiros de tecnologia.
- ✓ Autenticação, criptografia em trânsito e em repouso nos bancos de dados;
- ✓ Proteção contra softwares maliciosos em todas as estações de trabalho e nos servidores;
- ✓ Gestão e Detecção de Vulnerabilidades;
- ✓ Testes de Invasão;
- ✓ Busca e Antecipação de Ameaças e Ataques Cibernéticos;
- ✓ Segurança de Aplicações (Secure Coding);
- ✓ Controles de Acesso;
- ✓ Segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações; e
- ✓ Filtros de Conteúdo.

Registro, Resposta e Tratamento de Incidentes de Segurança Cibernética

O registro, resposta, ação e tratamento de incidentes de segurança da informação e cibernética devem ser realizados por meio de nosso formulário padrão. Uma cópia do registro está anexada ao final desta política e estará disponível em nossa intranet para as pessoas responsáveis pelo tema.

Classificação da relevância dos ativos e dos incidentes cibernéticos

A classificação consiste em verificar previamente, através de análise de impactos dos riscos, o grau de tolerância de paradas oriundos de ataques e o custo de parada. Quanto maior o custo de parada e menor o grau de tolerância as paradas causadas por ataques, maior criticidade será dada ao ativo-alvo. Além das classificações dos incidentes, a caracterização dos ativos é parte integral do processo de gestão de riscos cibernéticos. É nesta etapa que são identificadas as limitações, os recursos e as informações do ativo.

As caracterizações dos ativos são feitas pela área de gestão de riscos junto a Infraestrutura de sistemas. Nesta fase, são levantados:

- ✓ Informações de hardwares e softwares;
- ✓ Usuários que fazem uso do ativo;
- ✓ Missão do ativo, descrevendo os processos realizados por ele;
- ✓ Sensibilidade e criticidade do ativo;
- ✓ Políticas de segurança;
- ✓ Controles operacionais; e
- ✓ Relatórios Gerenciais.

Identificação de ameaças

As possíveis ameaças aos ativos de tecnologia são levantadas durante a análise de riscos e impactos. Para maior detalhamento, verificar o anexo I e a matriz de riscos de segurança cibernética.

Origem e Registro dos Alertas dos Incidentes Cibernéticos

Atividades suspeitas ou incidentes identificados por colaboradores ou terceiros devem ser comunicados imediatamente para a equipe de infraestrutura de sistemas, por meio da chave de emails infra@njpartners.com.br, com cópia para a chave de compliance no email compliance@hemeradtvm.com.br. Em caso de inacessibilidade de emails, os colaboradores, prestadores de serviços e clientes podem entrar em contato por meio do telefone corporativo.

Cada evento é gerenciado e respondido por diretrizes específicas que descrevem as tarefas necessárias em cada cenário de alerta. Para maior detalhamento dos alertas e tipos de incidentes, é necessário acessar o manual de procedimentos de tecnologia, no capítulo recuperação de desastre e resposta a incidentes cibernéticos.

Provedores e fornecedores que armazenam e processam dados, contratados pela Hemera, devem reportar os incidentes cibernéticos através do canal infra@njpartners.com.br, com cópia para a chave de compliance, além de seguir as diretrizes descritas nesta política.

Prevenção a Incidentes Cibernéticos

Threat Intelligence: Nada mais são do que indicadores estruturados e geridos pela área de segurança da informação, o que permite que os times de infraestrutura da Hemera possam obter informações referentes à possíveis riscos cibernéticos, ameaças, fraudes e incidentes cibernéticos, gerando planos de ação preventivos a partir destas informações. Todos os colaboradores da Hemera DTVM são treinados para reportarem quaisquer eventos ou comportamentos estranhos que possam acarretar riscos a nós e a continuidade do negócio.

Cenários de Incidentes Cibernéticos na Gestão de Continuidade de Negócios

Em caso de materialização dos cenários críticos descritos em nossa política de Gestão de continuidade de Negócios, o responsável direto pela segurança da informação e cibernética deve acionar imediatamente a área de Compliance e Gestão de riscos, que irá deliberar pelo acionamento do:

- ✓ **Planos de Continuidade de Negócios:** A comunicação e instauração de medidas de contingência deve ser realizada em cenários que ofereçam impacto significativo ao negócio, impactando ou inviabilizando a continuidade operacional e o uso das aplicações por terceiros.
- ✓ **Plano de Recuperação de Desastre (PRD):** A comunicação deve ser realizada em cenários particularmente sensíveis que ofereçam impacto à infraestrutura tecnológica da organização, impactos para a continuidade dos negócios internamente e para terceiros que acessem nossas aplicações.

Violação

Os princípios de Segurança Cibernética estabelecidos nesta política são endossados por nossos executivos e devem ser observados por todos.

As violações de segurança devem ser informadas ao gestor imediato e, simultaneamente, à área de infraestrutura de sistemas, que deverá tomar as providencias necessárias junto aos diretores. Toda violação ou desvio às diretrizes desta política será investigado para determinação das medidas cabíveis.

O não cumprimento de algum ponto desta política, intencional ou não, pode levar o funcionário, o estagiário ou o prestador de serviço a sanções disciplinares ou legais, dependendo do caso.

Vigência e Revisões:

O presente documento entra em vigor na data de sua publicação e será revisado no período máximo de um ano ou havendo necessidade anterior, o que for menor, para que o permaneça sempre atualizado.