POLÍTICA DE SEGURANÇA CIBERNÉTICA

Assunto: Resumo da Política de Segurança Cibernética	
Data de Emissão: 30/04/2019	**Data da última atualização:** 30/04/2019

Política de Segurança Cibernética ("Política")

1. Introdução

A Política visa definir os princípios e diretrizes de segurança cibernética e requisitos de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, adotados por esta Instituição e seus Colaboradores, na sua atuação interna ou externa.

A Política destina-se a todos os Colaboradores e terceiros envolvidos, direta ou indiretamente, nas operações e processos de negócios da Limine DTVM.

2. Definições

Colaborador(es): No âmbito desta Política, serão (i) os sócios e administradores da Instituição; (ii) os funcionários, sejam eles contratados por prazo determinado ou indeterminado, independente do cargo ou função; (iii) os estagiários e menores aprendizes; e, (iv) quaisquer outras pessoas físicas ou jurídicas que por força de relação empregatícia, trabalhista ou contratual com a Instituição prestem qualquer tipo de serviço e que possam ter acesso a alguma informação confidencial e/ou privilegiada.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Integridade: garantia da exatidão e integridade da informação e dos métodos de processamento.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Risco: qualquer evento que possa causar impacto na organização e seus objetivos do negócio.

Ameaça: evento ou atitude indesejável que potencialmente remove, desabilita, danifica ou destrói um recurso ou informação.

Vulnerabilidade: são definidas como a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Incidente: qualquer evento que não faz parte da operação normal de um serviço e que pode causar, ou causa, uma interrupção do serviço ou uma redução de sua qualidade.

Evento: é a ocorrência identificada em um sistema, serviço ou rede que indica uma possível violação da segurança da informação, ou uma situação desconhecida, que passa a ser relevante para a segurança dos ativos.

Cloud / Nuvem: rede integrada na internet que oferece serviços de computação com manutenção e recursos efetuados pela empresa contratada.

3. Objetivos

A Limine DTVM estabelece os princípios e diretrizes de segurança cibernética com os seguintes objetivos:

- Assegurar a confidencialidade, integridade e disponibilidade das informações próprias e de terceiros;
- Estabelecer medidas preventivas, detectivas e corretivas voltadas para o ambiente cibernético, reduzindo vulnerabilidades;
- Identificar e tratar potenciais incidentes;
- Garantir a continuidade dos negócios da Instituição;
- Treinar e conscientizar os Colaboradores sobre a segurança cibernética.

4. Procedimentos e Controles

A Limine DTVM estabeleceu procedimentos e controles para reduzir a vulnerabilidade da Instituição a incidentes e atender aos demais objetivos de segurança cibernética, dentre eles: controle de rastreabilidade, controle de acessos, cópias de segurança, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de informações, realização periódica de testes e varreduras, proteção contra software malicioso.

5. Registro e Análise da Causa e Impacto

A Instituição mantém registro de todas ocorrências e informações recebidas que sejam referentes a incidentes cibernéticos, que são analisadas e classificadas quanto a criticidade, bem como identificados as causas e impactos para a Instituição.

6. Diretrizes para a Segurança Cibernética

A Política contempla as diretrizes para a segurança cibernética, incluindo:

- Elaboração de Cenário de Incidentes: considerando os sistemas e ferramentas essenciais para a continuidade de seus negócios, combinada com as possíveis situações que seriam considerados incidentes relevantes para a Instituição.

- Prevenção e Tratamento de Incidentes: utiliza ferramenta de controle de ameaças através de monitoramento dos sistemas e rede corporativa, a fim de prevenir acessos não autorizados que possam comprometer a integridade e disponibilidade de seus serviços.

- Classificação dos Dados e Informações: as informações recebidas e geradas pela Instituição serão classificadas para que todos os Colaboradores tomem ciência e assim seja dado o adequado tratamento às referidas informações.

- Avaliação dos Incidentes: os incidentes após registrados e analisados, serão classificados de acordo com a relevância e impacto à Instituição.

7. Disseminação da Cultura de Segurança Cibernética

A Limine possui processo que visa conscientizar os usuários da necessidade da segurança das informações e aspectos previstos na Política de Segurança Cibernética.

A alta administração da Limine tem conhecimento da responsabilidade quanto a segurança cibernética, por este motivo, se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas recorrentes em Comitês internos da Instituição.

8. Compartilhamento de Informações sobre Incidentes Relevantes

A Instituição compartilhará as informações sobre os incidentes classificados com relevância alta, com os órgãos reguladores competentes e aptos a receber a informação, conforme regulamentação vigente.

9. Da Contratação de Terceiros para Serviços Relevantes

Com a finalidade de garantir a execução de controles para a prevenção de incidentes, a Instituição adota como procedimentos para a contratação de fornecedores de serviços de processamento e armazenamento de dados e de computação na nuvem, a análise de diversos aspectos do fornecedor, a fim de garantir que os mesmos possuam controles compatíveis com os adotados pela própria Instituição.

10. Vigência e Revisão anual

A Política é revisada no mínimo, anualmente pela Instituição, podendo ser realizada em periodicidade menor, caso seja necessário, em decorrência de exigência regulamentar ou legislação aplicável, o qual será elaborada pela área de Compliance, mediante de acordo da Diretoria da Instituição.