POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão 2019.1

Editada em Abril de 2019

SUMÁRIO

1. INTRODUÇÃO 3
2. OBJETIVOS 3
3. PROCEDIMENTOS E CONTROLES 4
4. REGISTRO E ANÁLISE DA CAUSA E IMPACTO 5
5. DIRETRIZES PARA ELABORAÇÃO DE CENÁRIOS DE INCIDENTES 5
6. PREVENÇÃO E TRATAMENTO DE INCIDENTES 5
7. CLASSIFICAÇÃO DOS DADOS E DAS INFORMAÇÕES 6
8. AVALIAÇÃO DE RELEVÂNCIA 6
9. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA 7
10. PROGRAMA DE CAPACITAÇÃO E DE AVALIAÇÃO PERÓDICA 7
11. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO 7
12. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES 8
13. DISPOSIÇÕES FINAIS 8
14. VIGÊNCIA E APROVAÇÃO 8

MENSAGEM DA DIRETORIA

Prezado colaborador,

Este documento tem como objetivo esclarecer e orientar quanto à segurança cibernética, sendo este complementar ao Código de Ética e Conduta.

Solicitamos que leia atentamente esta Política para entendimento e conhecimento das normas e diretrizes internas específicas para a segurança de cada área, sendo esta disponibilizada na intranet - sistema SCOT, aos que utilizam os sistemas informatizados da empresa, podendo ser impresso e ao conhecimento de todos, orientando e atribuindo as responsabilidades internas dos colaboradores.

Sendo assim, contamos com a colaboração de todos para a utilização íntegra e segura aos sistemas, internet e procedimentos internos da Oliveira Trust.

1. INTRODUÇÃO

A Política de Segurança Cibernética ("Política") da Oliveira Trust DTVM S/A foi criada para definir as diretrizes e demais especificações necessárias com a segurança cibernética, garantindo que suas informações e dados sejam administrados de maneira segura e responsável.

Esta Política se estende ainda a todos os colaboradores da Oliveira Trust Servicer S/A, doravante designadas em conjunto neste como "Oliveira Trust", devendo todos os colaboradores pautar a sua conduta em conformidade com os valores de boa-fé, ética, lealdade e veracidade e, ainda, pelos princípios gerais aqui estabelecidos.

Os clientes, investidores, visitantes ou demais, exceto os colaboradores da Oliveira Trust, são designados neste como, "*usuários*". São considerados "*colaboradores*", os estagiários e funcionários que trabalham na Oliveira Trust.

O Treinamento Admissional e o Código de Ética e Conduta que todo o colaborador faz na sua entrada na empresa são complementos a esta política e tem como objetivo agregar conhecimento e responsabilidade, devendo o colaborador assinar o Termo de Conhecimento.

2. OBJETIVOS

A Oliveira Trust estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

- Proteger o valor e a reputação da empresa;
- Garantir a confidencialidade, integridade e disponibilidade das informações próprias, e de terceiros por ele custodiadas, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;

- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias;
- Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

3. PROCEDIMENTOS E CONTROLES

A Oliveira Trust estabelece os principais procedimentos e controles adotados para reduzir a vulnerabilidade da instituição a incidentes:

- As informações próprias e dos clientes devem estar de acordo com as leis e normas internas vigentes, tratadas de forma ética e sigilosa;
- A informação deve ser utilizada conforme a classificação interna e somente para a finalidade ao qual foi coletada;
- O acesso às informações e recursos deverá ser realizado somente por pessoal devidamente autorizado;
- Os colaboradores deverão receber identificação única, pessoal e intransferível de modo que permita a identificação das ações realizadas no desenvolvimento de suas atividades profissionais;
- A concessão de acessos deve obedecer ao procedimento interno, com o objetivo de garantir que os usuários possuam acesso somente aos recursos de informação necessários para o desenvolvimento de suas atividades profissionais;
- A senha de acesso à rede corporativa e aos sistemas internos é de uso pessoal, sendo proibido seu compartilhamento;
- Os riscos relacionados à tratativa das informações devem ser reportados, imediatamente, à Diretoria;
- A proteção contra softwares maliciosos, bem como, o monitoramento periódico, devem obedecer a procedimento interno, com o objetivo de garantir a atualização da ferramenta, controle e solução dos eventos identificados;
- A realização de cópias de segurança (backups) deve obedecer ao procedimento interno, com o objetivo de garantir a realização e monitoramento das cópias de segurança;

- As ocorrências de problemas de software e/ou hardware, incluindo “helpdesk”, deverão obedecer ao procedimento interno, com o objetivo de garantir o registro e acompanhamento da solução.

4. REGISTRO E ANÁLISE DA CAUSA E IMPACTO

Toda ocorrência, bem como as informações recebidas de terceiros, deverá ser registrada em sistema interno e avaliada pela equipe de tecnologia da informação para a determinação da criticidade e impacto causados nas operações.

5. DIRETRIZES PARA ELABORAÇÃO DE CENÁRIOS DE INCIDENTES

A Oliveira Trust considera possíveis combinações, das variáveis críticas, para a elaboração dos cenários de incidentes. As variáveis críticas devem ser definidas com base nas necessidades relacionadas ao negócio, considerando os impactos no caso de utilização indevida dos dados e das informações.

6. PREVENÇÃO E TRATAMENTO DE INCIDENTES

A Oliveira Trust mantém softwares de controle de ameaças e vazamento de informações atualizados de acordo com as melhores práticas vigentes, a fim de se prevenir acessos não autorizados que possam comprometer sua integridade e disponibilidade de seus serviços.

Qualquer incidente ou falha em seus serviços internos deverão ser reportados, acompanhados, classificados e solucionados através de sistema interno que permita o compartilhamento entre os responsáveis pela segurança tecnológica, compliance e alta administração.

Prestadores de serviços que manuseiem dados ou informações sensíveis devem assinar o Termo de Prevenção e Tratamento de Incidentes fornecido pela Oliveira Trust e possuem obrigação de se reportar sobre eventuais incidentes que possam ter ocorrido assim como as devidas soluções para tratamento do problema e sua prevenção. Estas informações deverão ser acompanhadas e classificadas em sistema interno que permita o compartilhamento entre os responsáveis pela segurança tecnológica, compliance e alta administração.

7. CLASSIFICAÇÃO DOS DADOS E DAS INFORMAÇÕES

A Oliveira Trust estabelece o compromisso com o tratamento adequado das informações de seus clientes, visando:

- **Confidencialidade**: garantir que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;
- **Disponibilidade**: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- **Integridade:** garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

7.1. NÍVEIS DE CONFIDENCIALIDADE

Os dados e as informações devem ser classificados de acordo com a sua criticidade, com três níveis de confidencialidade: confidencial, uso interno e pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, compartilhamento ou restrição de acessos, bem como os impactos no caso de utilização indevida dos dados e das informações.

- **Confidencial:** informação sigilosa, de caráter estratégica, restrita a diretoria ou a quem for designado por esta;
- **Uso interno:** informação destinada para uso exclusivo da Oliveira Trust;
- **Pública:** informação destinada para o público em geral.

8. AVALIAÇÃO DE RELEVÂNCIA

Os incidentes são classificados da seguinte forma:

Crítica: Todo e qualquer incidente que possa comprometer a imagem da instituição e dados confidenciais dos seus clientes.

Alta: Todo e qualquer incidente que possa comprometer a disponibilidade de serviços e sistemas relevantes da organização, ou seja, aqueles que afetam o processamento de Custódia, Escrituração e liquidações.

Média: Todo e qualquer incidente relacionado a tentativas de acessos não autorizados e qualquer incidente que possa comprometer a disponibilidade de serviços e sistemas da organização não relevantes.

Baixa: Incidentes relacionados ao compartilhamento de informações não relevantes.

9. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

A Oliveira Trust promove a disseminação dos princípios e diretrizes de segurança cibernética através de programas de conscientização e treinamentos específicos, visando o fortalecimento da cultura interna de gestão de segurança da informação.

10. PROGRAMA DE CAPACITAÇÃO E DE AVALIAÇÃO PERÓDICA

A Oliveira Trust mantém política de treinamento e capacitação elegível a todos os colaboradores da empresa. A política é revisada anualmente, e tem por objetivo a capacitação e o desenvolvimento continuado de seus colaboradores.

11. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A alta administração contribui para o fortalecimento do Sistema de Controles Internos e da Segurança Cibernética, se comprometendo no mínimo, mas não se limitando as ações abaixo:

- Investir recursos necessários ao processo de prevenção de incidentes;
- Incentivar e praticar continuamente a disseminação de uma cultura de controles internos e de gestão de riscos;
- Manter colaboradores experientes, qualificados, motivados, continuamente treinados e comprometidos com suas atribuições e responsabilidades; com os objetivos e metas estabelecidos pela administração e com a prestação de serviços de qualidade; e
- Incentivar a segregação de funções nas diversas áreas envolvidas no processo de prestação desses serviços.

12. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES RELEVANTES

Os incidentes classificados com relevância alta/crítica deverão ser reportados aos órgãos reguladores competentes e aptos a receber a informação no momento de sua detecção.

Adicionalmente, a equipe responsável pelo gerenciamento de incidentes deverá buscar ferramentas seguras e de ampla utilização pelo mercado para compartilhar com outras instituições os incidentes relevantes com o objetivo de impedir que o ato malicioso se espalhe.

O prazo mínimo para armazenamento das ocorrências, soluções e compartilhamento deverá ser de 5 anos.

13. DISPOSIÇÕES FINAIS

Esta Política é de uso restrito e interno à instituição e é expressamente vedada a sua comercialização, reprodução, modificação, divulgação, publicação ou distribuição, a qualquer título ou forma, da totalidade ou de parte das informações, disponibilizada na intranet da Oliveira Trust (SCOT - Manuais e Normas) sem a prévia e expressa autorização da Diretoria ou Gerência da Oliveira Trust.

14. VIGÊNCIA E APROVAÇÃO

Esta Política tem vigência de 1 (um) ano, devendo ser revisada e atualizada anualmente.

Versão	Data	Revisado/ Aprovado	Responsável
2019.1	08/04/2019	Revisado	Felipe Moraes / Ismar Marcos
2019.1	30/04/2019	Aprovado	Henrique Sismil
2019.1	30/04/2019	Aprovado	Alexandre Freitas

OLIVEIRA TRUST