POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão 2025.1

Editada em março de 2025

SUMÁRIO

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 Pessoais (conjuntamente “Informações”) sejam administrados de maneira segura e responsável em sistemas/internet. A Política complementa a Política de Segurança da Informação, as quais devem ser lidas e interpretadas em conjunto. Os termos grafados com as iniciais em maiúscula deverão ser interpretados a partir do glossário contendo termos definidos na Política de Segurança da Informação, salvo quando definidos de modo diverso neste documento.

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 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 e a exposição indevida de Informações:

- As Informações próprias, e dos Usuários e Colaboradores devem estar de acordo com as leis, normas e Políticas internas vigentes, tratadas de forma ética e sigilosa, em especial a Lei nº 13.709/2018 (“Lei Geral de Proteção de Dados” ou “LGPD”);
- A Informação deve ser utilizada conforme a classificação interna estabelecida na Política de Segurança da Informação e somente para a finalidade ao qual foi coletada, ou finalidades diversas, mas compatíveis com aquela que ensejou a sua coleta,

sempre conforme as orientações dos Gestores, do Encarregado de Proteção de Dados e da Diretoria;

- O acesso às Informações e recursos deverá ser realizado somente por pessoal devidamente autorizado, conforme privilégios de acesso aos sistemas de maneira proporcional àquilo que cada profissional estritamente possa e deva acessá-las para o desempenho de suas funções.
- 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. As autorizações só devem ser concedidas baseadas na necessidade de conhecimento ou uso regulado por cargo e função;
- 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, à TI e ao Encarregado de Proteção de Dados (no caso de risco envolvendo Dados Pessoais);
- 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. CLASSIFICAÇÃO DOS DADOS E DAS INFORMAÇÕES

A Oliveira Trust estabelece o compromisso com o tratamento adequado das Informações dos Usuários, 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.

4.1. NÍVEIS DE CONFIDENCIALIDADE

As Informações devem ser classificadas 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.

5. 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.

No caso de Dados Pessoais, os registros de processos de tratamento deverão ser registrados no Inventário de Dados Pessoais (ou "RoPA", conforme detalhado na Política de Governança de Dados Pessoais), e o Encarregado deverá ser envolvido em situações de

Ameaça e Incidentes de Segurança da Informação que envolvam Dados Pessoais para que possa liderar a gestão do Incidente.

6. 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, na criticidade do teor das Informações objeto de incidente (ex. segredos de negócio, perda da confidencialidade de dados sensíveis, dados financeiros essenciais às operações da Oliveira Trust indisponíveis) considerando os impactos no caso de utilização indevida dos Dados Pessoais e Ias informações para os envolvidos.

Eventualmente, Incidentes de Segurança da Informação no meio cibernético podem ocorrer durante a condução regular das atividades da Oliveira Trust. Nestas situações, o importante é lidar de forma prática e objetiva, de forma a conter os danos e minimizar a exposição da Companhia, através de um planejamento prévio, orientado especificamente pela Política de Respostas a Incidentes e pela Política de Segurança da Informação.

7. 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, confidencialidade e disponibilidade de seus serviços.

As fases consideradas para gestão de um incidente, orientadas por uma Política de Resposta a Incidentes, serão: preparação, identificação, contenção, erradicação, recuperação e lições aprendidas (avaliação do processo de gestão de incidentes). Além disso, quando necessário, devem existir planos de continuidade e contingências que abranjam os sistemas de informação, de infraestrutura críticos e outros essenciais.

Os planos de continuidade do negócio serão focados nos riscos operacionais e alinhados com todos os planos de contingências e planos gerais da Oliveira Trust, ser testados regularmente para assegurar a adequação e seus funcionários compreendem a sua execução.

As notificações de Incidentes devem ser mantidas em registros e ter o detalhamento de todos os incidentes que forem gerados.

Prestadores de serviços que manuseiem Informações relevantes 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.

Além disso, a Oliveira Trust implementa as seguintes medidas para prevenção a ameaças de qualquer natureza à rede e sistema:

7.1. FILTRO DE CORREIO ELETRÔNICO (“E-MAIL”)

Todo o tráfego de E-mail de entrada e saída das caixas da Oliveira Trust é filtrado para proteger a Oliveira Trust contra ameaças que possam ser transmitidas por e-mail, além da proteção contra eventual vazamento de Informações.

7.2. FILTRO DE CONTEÚDO

O filtro de conteúdo usa a infraestrutura da internet para bloquear destinos maliciosos antes que uma conexão seja estabelecida entre esse destino e qualquer dispositivo conectado à rede da Oliveira Trust.

O filtro de conteúdo mitiga a atuação do Malware antes que ele alcance seus pontos finais ou rede. Mesmo que os dispositivos se infectem de outras maneiras, evita conexões com os servidores do invasor.

7.3. FIREWALL

O Oliveira Trust adota firewalls de última geração, que permitem analisar em tempo real a camada em que os softwares estão presentes, protegendo contra ameaças conhecidas e desconhecidas dentro de aplicações.

7.4. SOLUÇÃO ANTIVÍRUS

A Oliveira Trust pode usar soluções distintas conforme a necessidade e adequação para cada um dos equipamentos de rede, incluindo Data Centers, parque de computadores e demais dispositivos, com o objetivo de proteger conteúdo, baseado nas mais recentes tecnologias de mercado e atualizadas periodicamente.

7.5. MONITORAMENTO DO ACESSO À INTERNET

A Oliveira Trust entende que o uso da Internet é uma ferramenta valiosa para seus negócios, e um facilitador para as atividades desenvolvidas por todos os Colaboradores. Entretanto, o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade, sobre os Colaboradores e a própria reputação da Oliveira Trust.

Como medida protetiva e de acompanhamento, o Oliveira Trust monitora permanentemente o volume de tráfico na internet e na rede

7.6. LOGS

Os logs são registros cronológicos de atividades do sistema que possibilitam a reconstrução, revisão e análise dos ambientes e atividades relativas a uma operação, procedimento ou evento, acompanhados do início ao fim.
Os logs são utilizados como medidas de detecção e monitoramento, e registram atividades, falhas de acesso (tentativas frustradas de logon ou de acesso a recursos

protegidos) ou uso do sistema operacional, utilitários e aplicativos, com informação sobre o que foi acessado, por quem e quando.

Com os dados dos logs, pode-se identificar e corrigir falhas da estratégia de segurança cibernética, por conterem informações essenciais à detecção de acesso.

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, Encarregado de Proteção de Dados Pessoais e alta administração.

7.7. USO DE SENHAS

Os Usuários e Colaboradores devem seguir as boas práticas de segurança da informação na seleção e uso de senhas, conforme diretrizes constantes da Política de Segurança da Informação.

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.

Especificamente com relação a Incidentes envolvendo Dados Pessoais, a aferição quanto à sua criticidade deve considerar Risco ou dano relevante ao titular, para avaliação quanto à necessidade de comunicação do ocorrido à ANPD e ao titular do Dado Pessoal. O detalhamento quanto aos critérios e procedimentos adotados em caso de Incidentes deverá ser consultado em Política de Resposta a Incidentes.

9. MEIOS ELETRÔNICOS SEGUROS PARA ENVIO E RECEPÇÃO DE INFORMAÇÕES

A Oliveira Trust utiliza a plataforma de mensagens Google Workspace for Business para a troca de e-mails corporativos, estando as mensagens trafegadas por meio desta ferramenta sujeitas as regras de Compliance (filtros por palavras chaves), bem como sendo os e-mails com conteúdo indevido rejeitados automaticamente.

Existe também monitoramento através de compartilhamento das mensagens para os Colaboradores pertencentes ao mesmo grupo ou setor, sendo o acesso de envio e recepção de e-mails parametrizado de acordo com perfis de acesso pré-definidos para os Usuários.

Para a transferência de arquivos eletrônicos através de canal seguro, deve-se utilizar preferencialmente as ferramentas de trocas de arquivo a seguir em sua respectiva ordem de prioridade:

- Bucket - AWS
- IBM Connect:Direct
- WinSCP
- Filezilla (SFTP)

10. 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.

11. PROGRAMA DE CAPACITAÇÃO E DE AVALIAÇÃO PERIÓDICA

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.

12. 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.

13. 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. Especificamente com relação a Incidentes que envolvam Dados Pessoais, além da comunicação à ANPD, os titulares de Dados Pessoais deverão ser comunicados, desde que possam acarretar Risco ou dano relevante aos titulares.

O detalhamento quanto ao procedimento adotado em caso de Incidentes deverá ser consultado em Política de Resposta à Incidentes.

A ANPD recomenda que a comunicação de incidentes de segurança seja feita o mais breve possível, em até 2 (dois) dias úteis da ciência do fato.

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.

14. APROVAÇÃO

Esta Política deve ser revisada e atualizada anualmente.

Versão	Data	Revisado/ Aprovado	Responsável
2025.1	01/03/2025	Revisado	Gerente de Compliance
2025.1	01/03/2025	Revisado	Gerente - TI
2025.1	24/03/2025	Aprovado	Diretoria - TI
2025.1	24/03/2025	Aprovado	Diretoria – CEO

OLIVEIRA TRUST

TERMO DE PREVENÇÃO E TRATAMENTO DE INCIDENTES

1. Objetivo.

O presente Termo de Prevenção e Tratamento de Incidentes ("Termo") estabelece diretrizes para a prevenção, detecção e tratamento situações ("Incidente de Segurança da Informação") que possam comprometer a segurança, confidencialidade, disponibilidade e integridade de informações, sistemas e recursos da Oliveira Trust, incluindo dados pessoais, segredos de negócio, informações confidenciais (conjuntamente, "Informações"), que são tratados ou acessados pelo prestador de serviço e/ou parceiro ("Fornecedor") da Oliveira Trust, que subscreve este Termo.

O Fornecedor declara que implementa, minimamente, as medidas a seguir previstas, que são condição para a manutenção desta relação, estendendo-as a eventuais subcontratados, se aplicável, sem prejuízo das disposições contratuais que regem o relacionamento entre a Oliveira Trust e o Fornecedor.

2. Procedimentos de prevenção e tratamento.

O Fornecedor declara que mantém softwares de controle de ameaças e vazamento de informações atualizados de acordo com as melhores práticas vigentes, a fim de prevenir e impedir acessos não autorizados que possam comprometer sua integridade, confidencialidade e disponibilidade de seus serviços.

Além disso, o Fornecedor declara que implementa, minimamente, as seguintes medidas para prevenção a ameaças de qualquer natureza à rede e sistema:

2.1. Filtro de correio eletrônico ("e-mail")

Todo o tráfego de e-mail de entrada e saída das caixas do Fornecedor é filtrado para proteger o Fornecedor contra ameaças que possam ser transmitidas por e-mail, além da proteção contra eventual vazamento de Informações.

2.2. Filtro de conteúdo

O filtro de conteúdo usa a infraestrutura da internet para bloquear destinos maliciosos antes que uma conexão seja estabelecida entre esse destino e qualquer dispositivo conectado à rede do Fornecedor.

O filtro de conteúdo mitiga a atuação do Malware antes que ele alcance seus pontos finais ou rede. Mesmo que os dispositivos se infectem de outras maneiras, evita conexões com os servidores do invasor.

2.3. Firewall

O Fornecedor adota firewalls de última geração, que permitem analisar em tempo real a camada em que os softwares estão presentes, protegendo contra ameaças conhecidas e desconhecidas dentro de aplicações.

2.4. Solução antivírus

O Fornecedor usa soluções distintas conforme a necessidade e adequação para cada um dos equipamentos de rede, incluindo *Data Centers*, parque de computadores e demais dispositivos, com o objetivo de proteger conteúdo, baseado nas mais recentes tecnologias de mercado e atualizadas periodicamente.

2.5. Monitoramento do acesso à internet

Como medida protetiva e de acompanhamento, o Fornecedor monitora permanentemente o volume de tráfego na internet e na rede para identificação de comportamento atípico/ suspeito e toma as medidas preventivas aplicáveis para estancar eventuais riscos de forma tempestiva.

2.6. Logs

O Fornecedor retém registros cronológicos de atividades do sistema que possibilitam a reconstrução, revisão e análise dos ambientes e atividades relativas a uma operação, procedimento ou evento, acompanhados do início ao fim (“Logs”).

Os Logs são utilizados como medidas de detecção e monitoramento, e registram atividades, falhas de acesso (tentativas frustradas de login ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, com informação sobre o que foi acessado, por quem e quando.

Com os dados dos Logs, pode-se identificar e corrigir falhas da estratégia de segurança cibernética, por conterem informações essenciais à detecção de acesso.

2.7. Uso de senhas

Os usuários e colaboradores devem seguir as boas práticas de segurança da informação na seleção e uso de senhas, adotando política de senhas que impeça a utilização de senhas fracas e reforce a necessidade de sua confidencialidade e modificação periódica.

2.8. Outras medidas

Além das medidas de segurança cibernéticas que são adotadas, o Fornecedor declara que atua na prevenção de Incidentes de Segurança da Informação através da execução das seguintes medidas:

- Política de Segurança da Informação - com diretrizes de Segurança da Informação para o devido uso de sistemas, proibindo, por exemplo, baixar softwares indevidos pelos colaboradores do Fornecedor, com sanções possíveis de serem aplicadas caso exista um desrespeito à política;

- Análise de Risco - executar de forma periódica uma análise de risco de sistemas e aplicações.

- Segurança de host - executar processo de *hardening*, ou seja, *baseline* de configuração segura tanto no sistema operacional quanto nas aplicações dos hosts, sendo o processo revisado periodicamente.

- Segurança da rede - configurar o perímetro de rede para negar todas as atividades não permitidas, sendo o processo revisado periodicamente.

- Prevenção contra malware - uso de software para detectar e bloquear o malware a nível de *endpoint* (servidores e estações de trabalho), a nível de aplicação, tanto na parte servidor (servidor de e-mail e proxy web) quanto na parte cliente (cliente de e-mail e *instant message clients*). Importante a revisão das boas práticas configuradas na ferramenta de forma periódica.

- Treinamento e conscientização periódica dos seus colaboradores abordando boas práticas de segurança em sistemas (tais como uso de senhas e ativação do Múltiplo Fator de Autenticação - MFA), na rede (e-mail e internet), no ambiente físico, assim como nas diretrizes de segurança da informação interna do Fornecedor. O treinamento deve abordar o panorama legal da privacidade e proteção de dados no Brasil, melhores práticas, além de formas de identificar vulnerabilidades e atividades suspeitas.

3. Plano de Resposta a Incidentes

O Fornecedor declara possuir Plano de Resposta a Incidentes e de continuidade dos negócios.

Qualquer Incidente de Segurança da Informação, concreto ou suspeito, envolvendo as Informações da Oliveira Trust deverá ser registrado, reportado (se aplicável), acompanhado, classificado quanto a sua criticidade e solucionado conforme Plano de Resposta a Incidentes do Fornecedor, garantindo a implementação de medidas de mitigação e contenção pertinentes ao incidente em questão.

4. Comunicação de Incidentes.

Em caso do Fornecedor tomar conhecimento sobre a ocorrência (ou suspeita de ocorrência) de qualquer Incidente de Segurança da Informação envolvendo dados pessoais tratados no contexto de atividades desempenhadas e relacionadas com a Oliveira Trust, o Fornecedor deve informar à Oliveira Trust, por escrito, em até 24 horas a contar do conhecimento do evento, por meio do canal de contato dpo@oliveiratrust.com.br, informando detalhes sobre o incidente, a natureza dos dados pessoais afetados, os titulares afetados, os riscos relacionados, bem como as medidas de segurança para a proteção dos dados, soluções para tratamento do problema e mitigação dos prejuízos adotados antes e depois do incidente.

No caso dos incidentes acima referidos, o Fornecedor deverá cooperar com a Oliveira Trust no âmbito de qualquer investigação, seja ela realizada pela própria Oliveira Trust ou por profissionais externos, ou mesmo em qualquer processo judicial ou administrativo, assim como

adotará todas as medidas que forem solicitadas pela Oliveira Trust para mitigação e remediação de incidentes.

5. Auditoria.

O Fornecedor tem ciência de que a Oliveira Trust poderá a qualquer momento solicitar informações que comprovem as medidas de segurança tomadas para atendimento a este termo, assim como também poderá solicitar informações complementares que possam apoiar o entendimento de evidências enviadas.

6. Vigência.

Este Termo entra em vigor na data de assinatura e permanecerá em vigor durante a vigência do contrato entre o Fornecedor e Oliveira Trust ou enquanto o Fornecedor mantiver Informações da Oliveira Trust (o prazo que for maior).

Rio de Janeiro, [=] de [=] de 2025.

_____

[=]