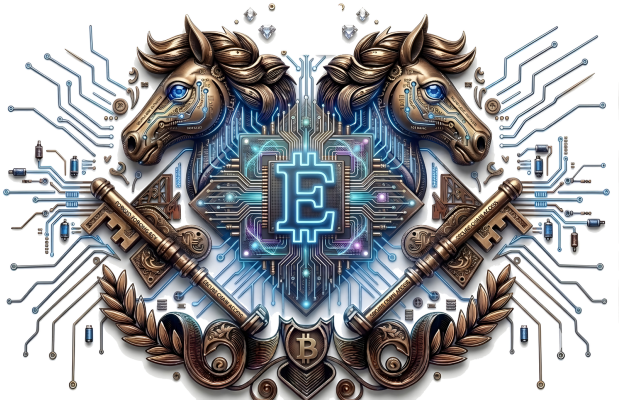

E.TA.NA CUSTÓDIA

INSTITUTIONAL DIGITAL ASSET CUSTODY TECHNOLOGY

DECLARAÇÃO INSTITUCIONAL · INSTITUTIONAL STATEMENT

Declaração de Segurança da Informação

Resumo público do programa de controles

Este documento descreve, em nível institucional, a natureza dos controles de segurança da informação adotados pelo Grupo e a fronteira técnica que delimita o acesso da E.TA.NA Custódia a chaves criptográficas e a ativos de clientes. Não descreve configurações, ferramentas ou procedimentos específicos.

DOCUMENTO	VERSÃO	EMISSÃO	REVISÃO	IDIOMA
ETC-COMP-2026/ DSI-001	**1.0**	**18/07/2026**	**Anual**	**Português (prevalece)**

Decorre da Política de Segurança da Informação e Cibernética ETC-COMP-2026/PSI-001
Canal de segurança: compliance@etanacustodia.com
Jet Privé Gestora de Fundos Ltda. (E.TA.NA Custódia) · CNPJ 58.367.528/0001-83
J.P. Gestora de Fundos Ltda. · CNPJ 40.243.371/0001-19

1 Compromisso e escopo

As entidades do grupo econômico J.P. Gestora de Fundos Ltda., entre as quais a Jet Privé Gestora de Fundos Ltda., que opera sob o nome comercial E.TA.NA Custódia, mantêm programa formal de segurança da informação e cibernética, aprovado pela administração e revisto ao menos anualmente.

O programa tem por objetivo preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade da informação e dos ativos tecnológicos, e sustentar tecnicamente os compromissos assumidos perante as instituições contratantes.

Este documento resume a natureza dos controles adotados. Não descreve configurações, ferramentas, topologias ou procedimentos específicos, cuja divulgação ampliaria a superfície de ataque. A documentação completa é disponibilizada a contrapartes institucionais em processo de diligência, mediante acordo de confidencialidade.

2 Fronteira técnica

DELIMITAÇÃO

A E.TA.NA Custódia não detém, não controla e não acessa chaves criptográficas de clientes, e não recebe nem movimenta ativos ou recursos de clientes. A custódia qualificada é prestada por custodiante autorizado, contratado direta e autonomamente pela instituição cliente.

A camada tecnológica situa-se entre os sistemas da instituição contratante e a infraestrutura do custodiante qualificado por ela contratado. Transporta instruções e dados operacionais. A autorização e a assinatura de operações ocorrem fora do perímetro da E.TA.NA Custódia.

Elemento	Situação
Chaves criptográficas de clientes	Fora do perímetro
Credenciais capazes de movimentar ativos de clientes	Fora do perímetro
Recursos financeiros e ativos virtuais de clientes	Fora do perímetro
Dados de instrução, posição e reconciliação	Dentro do perímetro, tratados na condição de operadora
Registros técnicos e trilhas de auditoria	Dentro do perímetro

Esta delimitação não é apenas declaratória. É sustentada por segregação de ambientes, controle de acesso por perfil, trilhas de auditoria e verificação independente, e é objeto de reatestação sempre que houver alteração material de arquitetura.

3 Domínios de controle

Domínio	Natureza dos controles adotados
Identidade e acesso	Menor privilégio e necessidade efetiva; identidades nominais; contas administrativas segregadas das contas de uso ordinário; revisão periódica formal de acessos; revogação no desligamento
Autenticação	Autenticação multifator obrigatória para consoles de infraestrutura, repositórios de código, acesso remoto, correio corporativo e sistemas que processem informação confidencial, com preferência por fatores resistentes a phishing. Requisitos de credenciais alinhados às diretrizes internacionais vigentes de identidade digital
Criptografia	Cifragem em trânsito e em repouso; cifragem integral de disco em estações e dispositivos; segredos de aplicação custodiados em cofre e nunca em código-fonte
Desenvolvimento	Segregação entre ambientes de desenvolvimento, homologação e produção; revisão de código por pessoa distinta do autor; verificações automatizadas de segurança no fluxo de integração; controle e reversibilidade das promoções a produção
Infraestrutura	Configuração segura por padrão; segmentação de rede e restrição de exposição pública; restrição de acesso administrativo por lista de endereços autorizados; monitoramento de eventos de infraestrutura

Domínio	Natureza dos controles adotados
Registros e auditoria	Trilhas de auditoria protegidas contra alteração, sincronizadas em tempo universal coordenado, segregadas das funções que as geram
Vulnerabilidades	Varredura periódica; acompanhamento contínuo de dependências de terceiros; classificação por severidade com prazos de correção definidos; aceitação de risco residual em caráter excepcional, temporário e aprovado
Terceiros	Avaliação de segurança prévia à contratação, proporcional ao risco; cláusulas de proteção de dados, notificação de incidentes e evidências de auditoria; reavaliação periódica
Dados pessoais	Tratamento disciplinado pela Política de Privacidade e Proteção de Dados Pessoais do Grupo, com delimitação expressa das posições de controladora e de operadora

4 Verificação independente

O programa estabelece a submissão dos controles a verificação por terceiros sem vínculo com a operação, compreendendo avaliação independente de controles, teste de intrusão e revisão periódica de configurações críticas, com plano de ação documentado para as deficiências identificadas.

As evidências correspondentes, incluindo sumários de relatórios de teste e de avaliação, são disponibilizadas a contrapartes institucionais mediante solicitação em processo de diligência, na forma e na extensão previstas nos instrumentos contratuais.

O programa é referenciado às boas práticas internacionais de gestão de segurança da informação e de gestão de risco cibernético, adotadas em caráter proporcional ao porte e à complexidade das entidades. Esta referência não constitui, nem deve ser interpretada como, declaração de certificação.

5 Gestão de incidentes

O Grupo mantém processo formal de resposta a incidentes, com registro, triagem, classificação por severidade, contenção, erradicação, recuperação, comunicação e análise posterior de causa raiz.

Os incidentes são classificados em níveis de severidade, aos quais correspondem tempos de resposta definidos, formalizados nos instrumentos contratuais celebrados com cada instituição contratante. As instituições contratantes são comunicadas sem demora injustificada quando o incidente afetar os serviços prestados ou dados sob sua titularidade, em prazo que não comprometa o cumprimento, por elas, dos prazos regulatórios aplicáveis.

Quando houver dados pessoais afetados, aplicam-se os prazos e a disciplina da Política de Privacidade e Proteção de Dados Pessoais do Grupo, observada a distinção entre as posições de controladora e de operadora.

Todos os incidentes são registrados, inclusive os de baixa severidade e os que não ensejem comunicação externa.

6 Continuidade e resiliência

As informações e os ambientes críticos são objeto de cópias de segurança cifradas, armazenadas com segregação em relação ao ambiente de origem e submetidas a teste de restauração periódico com registro do resultado.

O Grupo mantém plano de continuidade de negócios e de recuperação de desastre, com identificação dos processos críticos, das dependências de terceiros, dos objetivos de tempo e de ponto de recuperação e dos procedimentos de acionamento. O plano é testado periodicamente, e o sumário do teste é disponibilizado às instituições contratantes na forma dos instrumentos contratuais.

7 Pessoas e cultura

Colaboradores, estagiários e prestadores com acesso a informações ou a recursos tecnológicos participam de programa anual e obrigatório de conscientização, que abrange fraude por mensagem eletrônica, engenharia social, personificação, gestão de credenciais, classificação da informação e comunicação de incidentes. Quem tem acesso a ambientes de produção ou a código-fonte recebe treinamento adicional em desenvolvimento seguro.

Todos assinam termo de confidencialidade cuja vigência sobrevive ao término do vínculo. A comunicação de boa-fé de incidente ou de suspeita não sujeita o comunicante a medida disciplinar pelo fato comunicado.

8 Governança do programa

Item	Definição
Instrumento	Política de Segurança da Informação e Cibernética ETC-COMP-2026/PSI-001
Aprovação	Administração das entidades abrangidas

Item	Definição
Responsável designado	Responsável por Segurança da Informação, com atribuição formal. É vedada a concentração das funções de execução e de verificação na mesma pessoa
Revisão ordinária	Anual
Revisão extraordinária	Alteração material de arquitetura; incidente de severidade crítica; achado de auditoria ou de teste de intrusão; alteração normativa aplicável
Documentos correlatos	Política de Prevenção à Lavagem de Dinheiro, Sanções e Integridade; Política de Privacidade e Proteção de Dados Pessoais

9 Comunicação de vulnerabilidades e contato

Pesquisadores de segurança, clientes e contrapartes que identifiquem vulnerabilidade ou fragilidade nos serviços do Grupo devem comunicá-la pelo endereço **compliance@etanacustodia.com**, com descrição suficiente à reprodução.

O Grupo compromete-se a acusar o recebimento, a avaliar a comunicação e a manter o comunicante informado sobre o encaminhamento. Solicita-se que a informação não seja divulgada publicamente antes da correção, e que a verificação não envolva acesso a dados de terceiros, degradação de serviço nem qualquer ação que exceda o necessário à demonstração da falha.

O mesmo endereço é o canal para solicitações de documentação de segurança em processos de diligência e para questões relativas a proteção de dados pessoais.

10 Security statement (English)

This section summarises the Group's information security posture. The Portuguese text prevails in the event of any divergence.

Scope. The entities of the J.P. Gestora de Fundos Ltda. group, including Jet Privé Gestora de Fundos Ltda., trading as E.TA.NA Custódia, maintain a formal information security and cyber programme approved by management and reviewed at least annually.

Technical boundary. E.TA.NA Custódia does not hold, control or access client cryptographic keys, and neither receives nor moves client assets or funds. Qualified custody is provided by an authorised custodian engaged directly and independently by the client institution. The platform sits between the contracting institution's systems and the custodian's infrastructure, carrying instructions and operational data; authorisation and signing occur outside the E.TA.NA Custódia perimeter. The boundary is supported by environment segregation, role-based access control, audit trails and independent verification, and is re-attested on material architectural change.

Controls. Least privilege with named identities and segregated administrative accounts; mandatory multi-factor authentication for infrastructure consoles, code repositories, remote access, corporate email and systems processing confidential information, favouring phishing-resistant factors; encryption in transit and at rest; secrets held in a vault and never in source control; segregated development, staging and production environments with mandatory peer code review and automated security checks in the pipeline; network segmentation and allow-listed administrative access; tamper-resistant audit trails in coordinated universal time; periodic vulnerability scanning with defined remediation deadlines; and risk-proportionate security assessment of third parties.

Assurance. Controls are submitted to independent verification by parties unconnected with operations, including independent controls assessment, penetration testing and periodic review of critical configurations, with documented remediation plans. Evidence, including report summaries, is made available to institutional counterparties on request during due diligence. The programme is referenced to international good practice in information security and cyber risk management, applied proportionately to the size and complexity of the entities. This reference does not constitute a claim of certification.

Incidents and resilience. A formal incident response process covers logging, triage, severity classification, containment, eradication, recovery, communication and root cause analysis. Response times by severity are formalised in contractual instruments. Contracting institutions are notified without undue delay where an incident affects the services or data under their control, within a period that does not prejudice their own regulatory deadlines. Encrypted, segregated backups are subject to periodic restoration testing, and a business continuity and disaster recovery plan is tested periodically.

Reporting a vulnerability. Please write to compliance@etanacustodia.com with sufficient detail to reproduce the issue. We will acknowledge receipt, assess the report and keep the reporter informed. We ask that findings not be published before remediation, and that testing avoid access to third-party data, service degradation or any action beyond what is necessary to demonstrate the issue.

Contact. compliance@etanacustodia.com. Version 1.0, dated 18 July 2026. Derived from Information Security and Cyber Policy ETC-COMP-2026/PSI-001.