



somos
natura

Manual do Fornecedor

Avaliação de Segurança Cibernética

natura



Objetivos

A avaliação de segurança tem como finalidade:

- **Assegurar** que fornecedores estejam alinhados aos padrões de Segurança da Informação da Natura;
- **Avaliar** o nível de maturidade dos controles de segurança implementados;
- **Identificar**, avaliar e mitigar riscos que possam impactar dados, sistemas e operações;
- **Promover** uma relação transparente, colaborativa e orientada à melhoria contínua.

natura

Na Natura, acreditamos que o cuidado com a segurança digital e continuidade de negócios é um compromisso compartilhado. Por isso, caminhamos lado a lado com nossos parceiros para garantir que todos estejam em sintonia com nossos padrões de cibersegurança. Este material foi criado para guiar você em cada etapa desse processo, de forma clara, segura e acessível.

Nosso propósito

Nossa Gestão de Riscos com Terceiros tem um foco principal: assegurar que nossos parceiros estejam totalmente alinhados com as práticas de segurança da Natura ao prestar seus serviços. É um processo colaborativo que nos ajuda a entender a maturidade dos seus controles de segurança, identificando e mitigando juntos quaisquer riscos que possam afetar os dados, sistemas e operações da Natura.

Escopo da *avaliação*

O escopo inclui a análise dos controles internos do fornecedor e dos seguintes domínios de risco:

- **Governança** de Segurança da Informação;
- **Privacidade** e Proteção de Dados;
- **Identidade** e Acessos;
- **Desenvolvimento** Seguro;
- **Inteligência** Artificial;
- **Monitoramento & Resposta** a Incidentes;
- **Proteção** da Infraestrutura & Cloud;
- **Riscos** & Continuidade;
- **Treinamento** e Conscientização;
- **Continuidade** de negócios e recuperação.

O escopo é dinâmico, pois pode ser ajustado durante a diligência com base nas respostas fornecidas no questionário e está sujeito à validação pelo time de Segurança da Informação Natura.



Visão geral do processo de avaliação

natura

01. **Classificação** do Serviço (tierização)

Nesta etapa, o responsável pelo fornecedor na Natura envia informações essenciais para classificação do fornecedor e do serviço prestado, considerando:

A	Tipo de dados envolvidos (dados pessoais, sensíveis ou confidenciais);
B	Criticidade do serviço para o negócio;
C	Envolvimento com processos estratégicos;
D	Desenvolvimento ou manutenção do sistema;

O prazo para realização da tierização e envio do questionário ao fornecedor é de até **3 dias úteis**.



02. **Resposta do questionário** e envio de evidências

Após a tierização realizada internamente pela Natura, o fornecedor receberá um questionário com questões sobre a segurança da informação do fornecedor.

O fornecedor deverá:



Responder integralmente ao questionário de segurança;



Garantir a veracidade e clareza das informações;



Anexar evidências obrigatórias que comprovem os controles declarados.

Respostas afirmativas sem evidências válidas serão consideradas como não conformes.

O prazo para resposta é de até 15 dias, considerando até 3 interações de cobrança, com prazos adicionais de 5 dias cada.

03. **Análise** técnica

A Natura realizará a análise das respostas e evidências com foco em:

- Governança e conformidade;
- Controles técnicos e organizacionais de segurança;
- Aderência às políticas e requisitos corporativos.

O prazo padrão de análise é de até **5 dias úteis**. Caso haja necessidade de complementação, o SLA será pausado e reiniciado após nova submissão.



04. **Plano** de ação

Quando aplicável, o fornecedor receberá:

- **Resultado** da avaliação e nota de conformidade;
- **Plano de ação** para mitigação de riscos identificados;
- **Prazos acordados** para implementação dos controles pendentes.

CrITÉrios de Classificação:

Categoria	Percentual de Gaps	Status
A	0% – 19%	Aprovação Direta
B	20% – 39%	Aprovação Direta
C	40% – 55%	Aprovação por Exceção
D	56% – 79%	Rejeição
E	80% – 100%	Rejeição

Os prazos para implementação dos planos de ação seguem a criticidade dos riscos:

Muito alto: até 2 meses
Alto: até 3 meses
Moderado: até 4 meses
Baixo: até 5 meses

05. **Responsabilidades** do fornecedor

O *fornecedor* compromete-se a:

- **Preencher** o questionário de forma completa e verdadeira;
- **Fornecer** evidências claras, organizadas e atualizadas;
- **Manter** coerência entre informações declaradas e documentos enviados;
- **Engajar** áreas internas relevantes (TI, Segurança, Jurídico, Privacidade);
- **Cumprir** os prazos estabelecidos;
- **Manter** canais de comunicação ativos durante todo o processo.

As evidências solicitadas podem incluir, mas não se limitam a:

- **Políticas** e normas internas;
- **Matrizes** de risco e relatórios de vulnerabilidade;
- **Procedimentos** de controle de acesso;
- **Evidências** de treinamentos e conscientização;
- **Documentação** de desenvolvimento seguro (DevSecOps);
- **Planos** de resposta a incidentes e continuidade;
- **Relatórios** de DPIA e governança de privacidade.

Declarações sem comprovação documental serão tratadas como **ausência de controle**.

Responsabilidade compartilhada

natura

A **proteção das informações e operações** é uma responsabilidade conjunta. A atuação colaborativa, transparente e contínua entre a Natura e seus fornecedores é **essencial** para garantir a segurança, a continuidade das operações e a conformidade legal.

Segurança é continuidade

O cumprimento destes requisitos fortalece a parceria, reduz riscos operacionais e contribui para a resiliência e competitividade do fornecedor no mercado.



Suporte e comunicação

Dúvidas relacionadas ao processo de avaliação devem ser direcionadas ao canal informado no convite de diligência ou para:

tprm_cyber@natura.net

natura





natura