
Bellinati
Perez
SERIEDADE,
COMPETÊNCIA
E INOVAÇÃO

Política de Fornecedores	
Código: BP01.09 **Versão:** 5.0 **Criação:** 30/07/2020 | **Última revisão:** 12/08/2025 **Tipo de documento:** Público	

1. INTRODUÇÃO

Para garantir a boa prestação do serviço dos fornecedores à Bellinati Perez é imprescindível diretrizes que orientem a boa gestão dos fornecedores.

Com isso o objetivo deste documento é:

- Estabelecer procedimentos para a adequação de Gestão de Fornecedores ao que tange a Lei Geral de Proteção de Dados – LGPD que permita identificar, analisar, gerenciar e monitorar os riscos operacionais decorrentes de produtos e serviços terceirizados.
- Avaliar o nível de exposição da Bellinati Perez aos riscos provenientes da contratação de Fornecedores, de maneira qualitativa:

    - Estabelecer critérios para avaliação do Nível de risco de Fornecedores, uma vez que as exigências de controle e avaliações a serem realizadas pela Bellinati Perez devem estar alinhadas ao risco que o Fornecedor representa para a organização;
    - Estabelecer os processos e atividades que viabilizam a gestão dos riscos operacionais inerentes à contratação de Fornecedores;
    - Definir os papéis e responsabilidades dos envolvidos.

2. ESCOPO DE APLICABILIDADE

Todos os colaboradores que sejam responsáveis por contratações de serviços terceirizados e os fornecedores da Bellinati Perez.

3. AVALIAÇÃO

As avaliações de Risco dos Fornecedores deverão ocorrer nos fornecedores que possuem produto e/ou serviço vigentes.

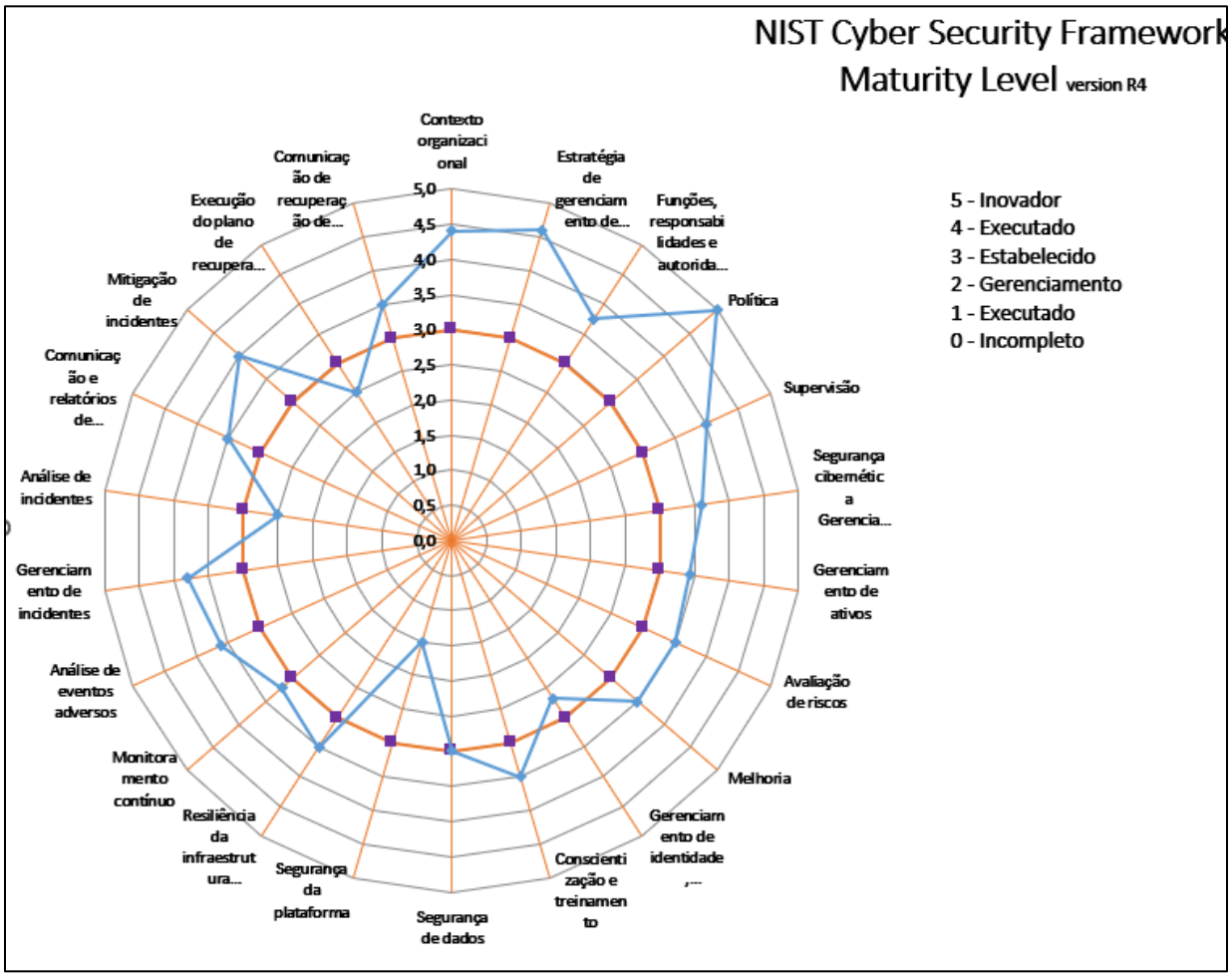
O primeiro passo é o preenchimento do Questionário de Avaliação Risco do Fornecedor, onde é feita a avaliação de criticidade do fornecedor quando a Segurança da Informação relacionada aos dados ou prestação de serviço realizada.

No questionário é encontrado na aba “Gráfico”, que após o preenchimento das questões de avaliação os controles de SI determinados serão classificados como:

- 0 – Incompleto
- 1 – Executado
- 2 – Gerenciado
- 3 – Estabelecido
- 4 – Previsível
- 5 – Inovador

Como maneira de metrificar a maturidade da postura de segurança do fornecedor avaliado, considerando a escala acima, são atribuídas notas de acordo com as respostas efetuadas no formulário de avaliação, sendo considerado como critério mínimo uma nota superior a 3 pontos. Caso o resultado dos itens avaliados fique com pontuação inferior a 3 pontos, a Bellinati Perez solicitará ao fornecedor um plano de ação ou plano compensatório para que a fragilidade detectada seja corrigida ou aprimorada.

Conforme exemplo abaixo:



O questionário disponibilizado ao fornecedor está baseado no framework NIST CSF 2.0 e preconiza avaliar todas as funções de segurança abaixo:

- Governança
- Identificar
- Proteger
- Detectar
- Responder
- Recuperar

A imagem abaixo representa as funções e categorias que são avaliados para cada fornecedor.

Função	Categoria	Identificador de categoria
Governar (GV)	Contexto organizacional	GV.OC
	Estratégia de gerenciamento de riscos	GV.RM
	Funções, responsabilidades e autoridades	GV.RR
	Política	GV.PO
	Supervisão	GV.OV
	Segurança cibernética Gerenciamento de riscos da cadeia de suprimentos	GV.SC
Identificar (ID)	Gerenciamento de ativos	ID.AM
	Avaliação de riscos	ID.RA
	Melhoria	ID.IM
Proteger (PR)	Gerenciamento de identidade, autenticação e controle de acesso	PR.AA
	Conscientização e treinamento	PR.AT
	Segurança de dados	PR.DS
	Segurança da plataforma	PR.PS
	Resiliência da infraestrutura tecnológica	PR.IR
Detetar (DE)	Monitoramento contínuo	DE.CM
	Análise de eventos adversos	DE.AE
Responder (RS)	Gerenciamento de incidentes	RS.MA
	Análise de incidentes	RS.AN
	Comunicação e relatórios de resposta a incidentes	RS.CO
	Mitigação de incidentes	RS.MI
Recuperar (RC)	Execução do plano de recuperação de incidentes	RC.RP
	Comunicação de recuperação de incidentes	RC.CO

3.1. AUDITORIA PERIÓDICA

A realização de auditorias nos fornecedores ativos é realizada anualmente, dentro da vigência do contrato, de modo a avaliar o nível de maturidade do fornecedor. Nos casos em que houve queda de maturidade ou foram identificados novos riscos, a auditoria deve envolver a área de negócios que poderá recomendar ações complementares ao fornecedor para se adequar aos padrões requeridos.

A escolha do mês em que a auditoria ocorre, em geral, ocorrera entre os meses de novembro e dezembro do ano vigente.

Dependendo do volume de fornecedores, as decisões indicam auditorias semestrais para os mais críticos, sendo definidos pelo volume de dados pessoais, confidenciais ou restritos tratados.

4. ANÁLISE E CLASSIFICAÇÃO DA CRITICIDADE DOS SEUS FORNECEDORES

Para garantir que os fornecedores da Bellinati Perez, cumpram as regras de Segurança e Privacidade de Dados, e protejam os dados pessoais dos clientes de seus clientes, necessário se faz, **a identificação e classificação da volumetria de dados pessoais disponibilizados a seus fornecedores,** analisando os seguintes passos:

a. Identificar os fornecedores críticos, ou seja, aqueles que têm acesso, tratam ou compartilham dados pessoais sensíveis, de crianças e adolescentes, ou que são transferidos internacionalmente. E ainda são fornecedores críticos, os que enriquecem dados, ou seja, que obtêm informações adicionais sobre os devedores, bem como os que enviam mensagens de SMS e de WhatsApp, na qual contém dados pessoais dos devedores fornecidos pela Bellinati Perez.

b. Classificar os fornecedores críticos de acordo com o nível de risco que representam para a segurança da informação e a privacidade de dados. Para isso, devem ser usados os critérios como o volume, a natureza e a finalidade dos dados tratados, as medidas técnicas e administrativas adotadas pelos fornecedores, o histórico de incidentes ou reclamações, entre outros. **Deverão ser usadas as escalas de baixo, médio e alto risco**.

c. Definir as ações a serem tomadas para cada fornecedor crítico, de acordo com o seu nível de risco. As ações podem incluir solicitar documentos, realizar auditorias se necessário, aplicar questionários, exigir garantias quando a demanda exigir, estabelecer cláusulas contratuais, monitorar o desempenho, entre outras. As ações devem visar assegurar que os fornecedores cumpram as normas da LGPD e respeitem os direitos dos titulares dos dados.

d. Atribuir as responsabilidades para cada ação, ou seja, definir quem vai executar, acompanhar e avaliar cada ação. As responsabilidades podem ser atribuídas aos gestores de área, ao encarregado de dados, ao setor jurídico, ao setor de compras, ou ao DPO. As responsabilidades devem ser claras e compatíveis com as competências de cada profissional ou setor.

e. Estabelecer os prazos para cada ação, ou seja, definir quando cada ação deve ser iniciada e concluída. Os prazos devem ser realistas e coerentes com a urgência e a complexidade de cada ação. Os prazos devem ser monitorados e atualizados conforme a evolução do plano de ação.

f. Alocar os recursos para cada ação, ou seja, definir quais são os meios materiais, financeiros e humanos necessários para a realização de cada ação. Os recursos devem ser suficientes e disponíveis para a execução do plano de ação. Os recursos devem ser gerenciados e otimizados conforme a necessidade de cada ação.

5. RELACIONAMENTO

A área responsável pela contratação fará todo o relacionamento com o fornecedor, no que se refere a negociação de valores, atualização de dados e documentos, comunicações de alterações pertinentes a Bellinati Perez etc.

A área responsável por contratos irá disponibilizar a relação de fornecedores ativos e a classificação de fornecedores críticos será determinada pela área de Privacidade e Proteção de Dados e compartilhada junto ao time de Segurança da Informação.

6. RESPONSABILIDADES

É responsabilidade dos Fornecedores cumprirem com o compromisso acordado pela prestação dos serviços firmados, assim como é recomendado aos fornecedores a busca constante pela qualidade prestada nos seus serviços e que os mesmos possuam um sistema de qualidade que possa ser verificado. Esses compromissos devem ser devidamente acordados em um contrato assinado entre as partes.

7. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Avaliar os Critérios de Conformidade do Fornecedor quando o nível de maturidade deste não for satisfatório no momento da contratação do fornecedor.

Avaliar os Critérios de Conformidade do Fornecedor quando houver queda de maturidade ou forem identificados novos riscos no momento da Auditoria.

8. TIME DE SEGURANÇA DA INFORMAÇÃO

Dar suporte para as áreas solicitante em caso de eventuais dúvidas técnicas no momento de análise do fornecedor.

Recomendar ações complementares para o fornecedor se adequar aos padrões requeridos em caso de queda de maturidade ou se forem identificados novos riscos no momento da Auditoria.

Enviar o Questionário de Avaliação dos Fornecedores ao Fornecedor.

9. PRESTAÇÃO DE CONTAS

A Bellinati Perez tem o dever de realizar a gestão dos fornecedores, acompanhando os serviços prestados, afinal é uma forma de controlar os mínimos controles de SI aplicados no ambiente dos fornecedores, dessa forma é possível analisar o resultado de acordo com o que foi estabelecido no contrato.

Dessa forma os fornecedores devem periodicamente informar a Bellinati Perez todas as atividades realizadas em determinado período, com a comprovação do cumprimento de cada uma delas e a Bellinati Perez deve realizar a validação dessas entregas.

10. GARANTIA DO ACORDO DE CONFIDENCIALIDADE

Por meio da NDA (acordo de não-divulgação) estarão firmados termo de confidencialidade a ser garantido por cada fornecedor. Em um contrato legal destacado o sigilo de informações confidenciais que as partes desejam restringir e compartilhar para determinado propósito. Bem como as penalidades caso ocorra algum incidente relacionados as informações confidenciais.

11. CONTROLE DE VERSÃO

Versão	Responsável	Data	Histórico de Atualizações
1.0	Joyce Ososki	30/07/2020	Proposição do documento
2.0	Time de Segurança	13/01/2022	Revisão da estrutura de documento
2.1	Time de Segurança	01/09/2022	Atualização para critérios de avaliação de fornecedores
3.0	Carlos Moreira	18/09/2023	Atualização de confidencialidade
4.0	Carlos Moreira	01/10/2024	Atualização nos termos de: avaliação, auditoria periódica, responsabilidades e prestação de contas.
4.1	Pio Carlos Freiria Jr	01/10/2024	Inclusão da Classificação de Criticidade
4.2	Douglas Ivanski da Silva	01/11/2024	Mudança de avaliação de fornecedores – Aplicação do Framework do NIST CSF 2.0
5.0	Roberto Godoi	12/08/2025	Revisão anual

12. APROVAÇÕES

	Responsáveis	Áreas	Datas
VALIDADO POR:	Jefferson Limeira	Gerente Executivo TI	15/08/2025
VALIDADO POR:	Paulo Henrique Ferreira	Diretor Executrivo	15/08/2025
APROVADO POR:	Luciano Reis	Superintendente Executivo TI	15/08/2025

13. CONTROLE DE COMUNICAÇÃO

TIPO DE COMUNICAÇÃO	O QUE COMUNICAR? (Assunto/Tema/Requisito)	QUANDO COMUNICAR? (Periodicidade)	COM QUEM SE COMUNICAR? (Partes Interessadas)	COMO COMUNICAR? (Meio de comunicação)	QUEM IRÁ COMUNICAR (Responsável)
Avaliação	Questionário de Avaliação	Anual	Área de fornecedores, DPO e Operações	Email, Sharepoint	Segurança