Bellinati Perez

Sumário

Política Corporativa Política de Fornecedores	
Código: BP02.16 **Versão:** 3.1 **Criação:** 30/07/2020 | **Última revisão:** 27/09/2023 **Tipo de documento:** Documento Oficial - Externo	Bellinati Perez

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.

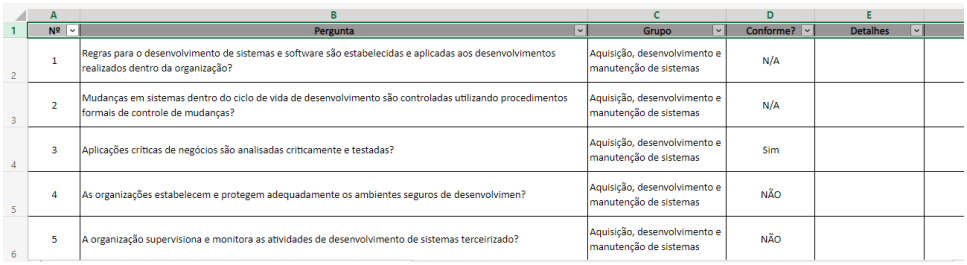
3. AVALIAÇÃO

As avaliações de Risco dos Fornecedores deverão ocorrer em dois momentos, sendo eles:

- Aquisição – Quando um novo produto e/ou serviço estiver em fase de negociação;
- Existente – Quando um produto e/ou serviço já pertence a DSBR, porém, necessita de uma avaliação periódica.

O primeiro passo é o preenchimento do Questionário de Avaliação Risco do Fornecedor, o qual foi elaborado pela própria Bellinati Perez e onde é feita uma pré-avaliação de criticidade do fornecedor, através dos campos da imagem abaixo. No questionário é encontrado na aba “Análise de Maturidade”. Após esta avaliação a maturidade do fornecedor, os pilares de SI definidos pelo NIST são classificados como: Inicial, Informal, Organizado, Otimizado, Gerenciado.

Conforme exemplo abaixo:

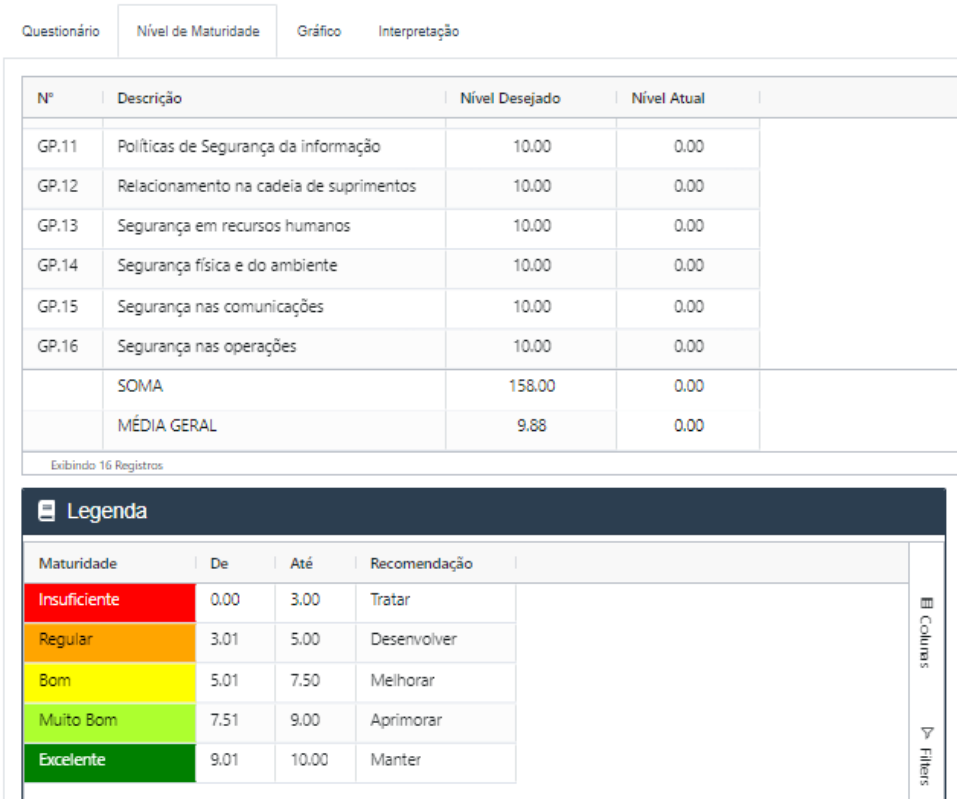


	A	B	C	D	E
1	Nº	Pergunta	Grupo	Conforme?	Detalhes
2	1	Regras para o desenvolvimento de sistemas e software são estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização?	Aquisição, desenvolvimento e manutenção de sistemas	N/A	
3	2	Mudanças em sistemas dentro do ciclo de vida de desenvolvimento são controladas utilizando procedimentos formais de controle de mudanças?	Aquisição, desenvolvimento e manutenção de sistemas	N/A	
4	3	Aplicações críticas de negócios são analisadas criticamente e testadas?	Aquisição, desenvolvimento e manutenção de sistemas	Sim	
5	4	As organizações estabelecem e protegem adequadamente os ambientes seguros de desenvolvimen?	Aquisição, desenvolvimento e manutenção de sistemas	NÃO	
6	5	A organização supervisiona e monitora as atividades de desenvolvimento de sistemas terceirizado?	Aquisição, desenvolvimento e manutenção de sistemas	NÃO	

O questionário enviado ao fornecedor está classificado nas dimensões abaixo:

- Aquisição, desenvolvimento e manutenção de sistemas
- Aspectos de SI na GCN
- Conformidade
- Controle de acesso
- Criptografia
- Equipamentos
- Físico
- Gestão de ativos
- Gestão de incidentes de SI
- Organização da segurança da informação
- Políticas de Segurança da informação
- Relacionamento na cadeia de suprimentos
- Segurança em recursos humanos
- Segurança física e do ambiente
- Segurança nas comunicações
- Segurança nas operações

Analise através dos relatórios abaixo:



Nº	Descrição	Nível Desejado	Nível Atual
GP.11	Políticas de Segurança da informação	10.00	0.00
GP.12	Relacionamento na cadeia de suprimentos	10.00	0.00
GP.13	Segurança em recursos humanos	10.00	0.00
GP.14	Segurança física e do ambiente	10.00	0.00
GP.15	Segurança nas comunicações	10.00	0.00
GP.16	Segurança nas operações	10.00	0.00
	SOMA	158.00	0.00
	MÉDIA GERAL	9.88	0.00

Maturidade	De	Até	Recomendação
Insuficiente	0.00	3.00	Tratar
Regular	3.01	5.00	Desenvolver
Bom	5.01	7.50	Melhorar
Muito Bom	7.51	9.00	Aprimorar
Excelente	9.01	10.00	Manter

E o gráfico de maturidade será compartilhado:

Nº	Descrição
GP.1	Aquisição, desenvolvimento e manutenção de sistemas
GP.2	Aspectos de SI na GCN
GP.3	Conformidade
GP.4	Controle de acesso
GP.5	Criptografia
GP.6	Equipamentos
GP.7	Físico
GP.8	Gestão de ativos

3.1. AVALIAÇÃO DE FORNECEDORES

No momento da aquisição de um novo produto ou serviço, é realizada uma análise técnica para auxiliar na seleção dos fornecedores através do Questionário de Análise do Fornecedor (seção 4.1) que será enviado juntamente com a RFP aos mesmos, neste é avaliado o nível de maturidade de cada um, o qual é analisado pela área contratante, no caso da análise apontar um nível de maturidade não satisfatório, esta irá para análise/aprovação do Comitê que após avaliação, irá informar se a contratação deve prosseguir ou se novos fornecedores devem ser procurados.

3.2. AUDITORIA PERIÓDICA

A realização de auditorias periódicas é também recomendada para os fornecedores com o contrato em andamento aplicando novamente o Questionário de Análise de Fornecedores, de modo a avaliar o nível de maturidade do fornecedor. Nos casos onde houve queda de maturidade ou foram identificados novos riscos, a auditoria deve envolver análise/aprovação do Comitê de Privacidade que poderá recomendar ações complementares do fornecedor para se adequar aos padrões requeridos.

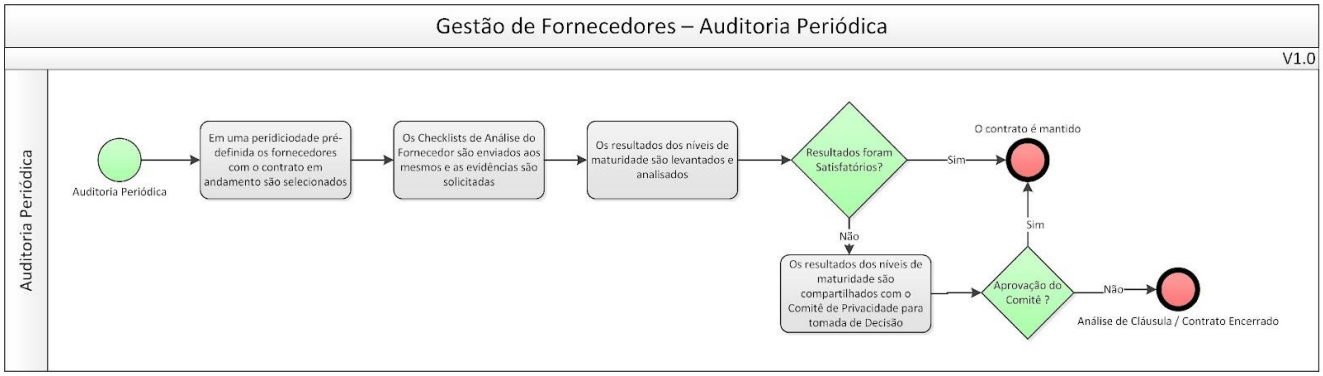
Por via de regra, as auditorias de LGPD nas empresas tem sido indicada como sendo de periodicidade anual, no mínimo.

A escolha do mês onde a auditoria ocorre, em geral, é antes do fechamento do orçamento do ano fiscal seguinte.

Dependendo do volume de fornecedores, as decisões indicam auditorias semestrais para os mais críticos.

De qualquer forma, a ANPD poderá determinar periodicidade mínima se entender necessário. No momento, não há qualquer orientação da Autoridade sobre periodicidade e a recomendação dada foi baseado no que o mercado pratica.

3.3. FLUXO



4. 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.

Estas condutas refletem no tipo de empresa que estamos contratando e na manutenção do bom relacionamento onde, dentre elas, temos:

- Contratação seguindo critérios profissionais e éticos;
- Manter boa reputação perante ao cliente, a comunidade e seus colaboradores;
- Praticar uma política de preços justos;
- Respeitar as legislações do País e o cumprimento de obrigações trabalhistas, ambientais, previdenciárias, fiscais e tributárias;
- Ser uma empresa preocupada com o bem-estar de seus colaboradores;
- Comprometimento com os acordos de confidencialidade;

5. RESPONSABILIDADES

É responsabilidade dos diretores e colaboradores da Bellinati Perez, quando responsáveis pela aprovação da contratação de Fornecedores, garantir o cumprimento desta Política e fazer uma boa gestão dessas contratações.

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.

5.1. 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.

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.

5.2. TIME DE SEGURANÇA DA INFORMAÇÃO

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

5.3. ÁREA DE FORNECEDORES

Enviar o Questionário de Avaliação dos Fornecedores ao Fornecedor no momento do envio da RFP.
Acompanhar a negociar com os Fornecedores os Valores Comerciais.
Enviar os Questionários de Análise de Fornecedores respondidos a Área Solicitante.

5.4. GARANTIA DO NÍVEL DE SERVIÇO

Por meio da SLA (Garantia do Nível de Serviço) estarão acordados os níveis de qualidade que devem ser garantidos a cada fornecedor, as responsabilidades e eventuais compensações quando os níveis de qualidade não forem atingidos. A fim de assegurar os direitos e deveres assumidos no que diz respeito exclusivamente as obrigações, além de servir como base para prever problemas que possam surgir no decorrer do negócio.

6. 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 a qualidade do serviço, porque uma vez que ele seja finalizado 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.

7. MULTA

Caso o Fornecedor não cumpra com o que foi combinado, a Bellinati Perez terá um respaldo jurídico para exigir seus direitos com base no que foi estabelecido em contrato.

O descumprimento do serviço prestado assim como a má qualidade poderão acarretar sérias consequências as atividades da Bellinati Perez. Por essa razão medidas como multas estarão inclusas de acordo com a gravidade dos prejuízos causados.

7.1. 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.

8. 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	Carlos Moreira	18/09/2023	Atualização de confidencialidade
3.1	Pio C. F. Jr.	27/09/2023	Revisão estrutural para atualização no site oficial

9. APROVAÇÕES

Responsáveis		Áreas	Assinaturas
VALIDADO POR:	Jefferson Limeira	TI	
VALIDADO POR:	Carlos Moreira	Segurança da Informação	
APROVADO POR:	Luciano Reis	TI	
APROVADO POR:	Pio Carlos Freiria Jr.	DPO	

10. 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