# PLANO DE AÇÃO GERAL PARA ADEQUAÇÃO À LGPD

## Escola Suíço Brasileira de São Paulo (ESB-SP) | Omnisblue

## Apresentação do projeto

O projeto associado a este documento trata da realização de ***atividades de assessoria visando a implementação de programa de adequação a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018) para as áreas de negócio da ESB – SP atendidas na primeira etapa do projeto (Recursos Humanos e Matrículas).***

## Objetivos do documento

- Documentar o resultado obtido após conclusão da etapa de **Preparação** do projeto de adequação à LGPD em execução na ESB – SP nas áreas atendidas pela primeira fase do projeto: Recursos Humanos e Matrículas.
- Direcionar os times da **Omnisblue** e **ESB - SP** em relação às atividades que precisam ser concluídas para finalizar a etapa de **Engajamento** e **Adequação** do projeto.

## Fundamentos legais

As análises e definições presentes neste documento estão fundamentadas na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18), nos parâmetros definidos pela norma ISO/IEC 27.001 e pelas estratégias definidas no framework de adequação à LGPD de propriedade da Omnisblue, apresentado para o time da **ESB - SP** ainda nas tratativas comerciais pré-projeto e, posteriormente, em maiores detalhes durante o *Workshop inicial sobre LGPD* já realizado no projeto.

Todas as ações sugeridas aqui têm como origem as informações fornecidas pelo Controlador durante a etapa de Preparação/Diagnóstico da Adequação à LGPD e essas informações estão todas inventariadas no ambiente *Privacy & Compliance Project (PCP)* do Controlador.

É imperativo que o Controlador e seus representantes tomem ciência das informações presentes na plataforma de governança de privacidade implementada (PCP) e, em caso de distorção em relação à realidade operacional de suas rotinas, alerte a Omnisblue, uma vez que as informações ali contidas foram fruto de levantamento e narrativas apresentadas pelos próprios representantes do Controlador.

## Resumo do projeto até aqui

O projeto de adequação à LGPD se iniciou com a elaboração do *Plano de Projeto* conhecido e firmado entre as partes e teve sua primeira ação mais palpável observável por todos os stakeholders com o *Workshop inicial sobre LGPD*.

A partir do alinhamento teórico entre as partes, foram realizadas diversas atividades de levantamento entre o time de especialistas da Omnisblue e os colaboradores do cliente (internos ou terceiros) onde foram levantados os aspectos *operacionais, tecnológicos* e *jurídicos* do Controlador relacionado às seguintes áreas de negócio:

- Recursos Humanos
- Matrículas

Esses levantamentos detalharam o escopo do projeto de acordo com os seguintes quantitativos inventariados:

- **28 processos de negócio**
  - Recursos Humanos: 09 processos
  - Matrículas: 11 processos
  - LGPD: 08 processos
- **28 ativos de informação**
- **117 artefatos contendo o uso de dados pessoais**
- **118 metadados pessoais em uso**
- **81 rotinas de tratamento de dados pessoais**
- **02 medidas administrativas de segurança (políticas)**
- **27 terceiros envolvidos nas rotinas de tratamentos de dados e/ou gestão de ativos de informação**
- **33 riscos de segurança e privacidade**
- **42 atividades de adequação a serem executadas nas etapas de Engajamento e Adequação**
  - Aspectos operacionais e administrativos: 23 ações
  - Aspectos tecnológicos: 15 ações
  - Aspectos jurídicos: 02 ações
  - Aspectos evolutivos: 02 ações

Todas as informações inventariadas, e disponibilizadas no ambiente de produção do *Privacy & Compliance Project (PCP)*, foram na sequência analisadas pelos especialistas da Omnisblue e, a partir dessa análise, foram elencados os *Riscos de Privacidade e Proteção de Dados Pessoais* associados ao escopo tratado no projeto e, a partir desses riscos, foram definidas as *Atividades de adequação* pendentes de execução para completar o ciclo de adequação do Controlador à Lei Geral de Proteção de Dados dentro dos limites de escopo do projeto.

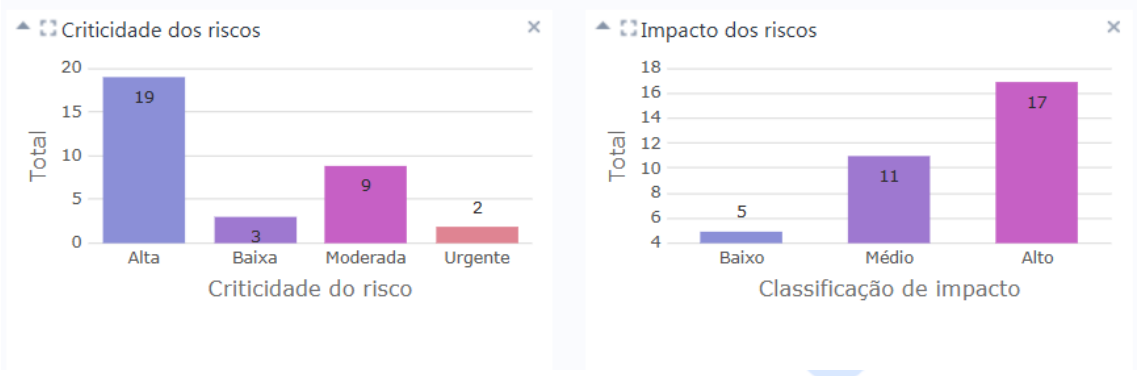
A seguir detalhamos então os *Riscos* e as *Atividades* definidas que endereçam as etapas de **Engajamento** e **Adequação** que passam a ser executadas a partir da aprovação deste documento.

## Visão geral dos riscos de privacidade e proteção de dados

Os riscos encontrados, inventariados e com suas respectivas estratégias definidas foram classificados de acordo com sua criticidade que é automaticamente observada de acordo com a seguinte matriz de classificação de impacto *versus* probabilidade:

| Probabilidade | Impacto: Baixo | Impacto: Médio | Impacto: Alto |
|---|---|---|---|
| 100% | Alta | Urgente | Urgente |
| 90% | Moderada | Urgente | Urgente |
| 80% | Moderada | Alta | Urgente |
| 70% | Moderada | Alta | Urgente |
| 60% | Moderada | Alta | Alta |
| 50% | Baixa | Alta | Alta |
| 40% | Baixa | Moderada | Alta |
| 30% | Baixa | Moderada | Moderada |
| 20% | Baixa | Baixa | Moderada |
| 10% | Baixa | Baixa | Moderada |

Esses riscos podem ser analisados em detalhe no ambiente PCP do Controlador, na funcionalidade "Riscos" e a distribuição de suas respectivas criticidades pode ser compreendida de acordo com o gráfico a seguir:




As atividades de adequação detalhadas a seguir tratam, inclusive, das ações a serem realizadas para executar as estratégias de gestão e monitoramento de todos os riscos inventariados pelo projeto até aqui.

A lista de riscos de privacidade deve ser compreendida como uma entidade que evolui ao longo do tempo, onde novos riscos serão descobertos, encerrados, disparados ou terão seus atributos modificados de acordo com eventos internos ou externos ao Controlador. A gestão desses riscos, muito além das atividades definidas neste plano, deve ser tarefa contínua, a ser realizada pelo DPO do Controlador durante a fase de **Operação** do ciclo de vida do Sistema de Gestão de Privacidade e Proteção de Dados (SGPD).

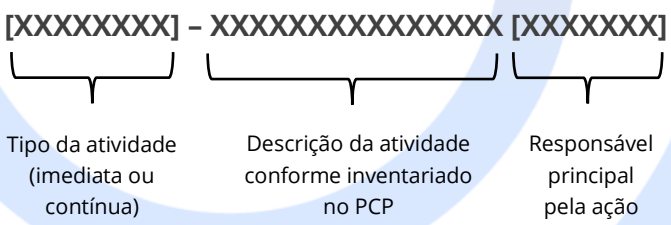
## Visão geral das ações de adequação a serem realizadas

As análises sobre todas as informações inventariadas durante a etapa de **Preparação** geraram uma lista de ações/atividades a serem executadas a seguir no projeto.
Essas atividades foram cadastradas no ambiente PCP do Controlador na funcionalidade “Atividades e Ações”.

Essas atividades podem ser classificadas de acordo com os aspectos de sua natureza técnica predominante, tal como segue:

- **Aspectos operacionais e administrativos:** Tratam de ações que alteram rotinas operacionais e administrativas do Controlador, adequando aspectos geralmente mais associados a papéis e responsabilidades, medidas administrativas e fluxo de informação e processos;
- **Aspectos tecnológicos:** Tratam de ações que alteram requisitos de Tecnologia da Informação do Controlador, adequando aspectos geralmente mais associados parâmetros de TI de Ativos de Informação eletrônicos e medidas técnicas de segurança;
- **Aspectos jurídicos:** Tratam de ações que alteram parâmetros jurídicos, legais e/ou contratuais do Controlador, adequando aspectos geralmente mais associados a contratos, bases legais, autorizações e responsabilidades legais;
- **Aspectos evolutivos:** Tratam de sugestões para se expandir a abrangência do SGPD em implantação para outras áreas ou departamentos do Controlador, bem como detalhar ainda mais as rotinas operacionais em busca de informações que porventura não foram detectadas durante as rotinas de levantamento realizadas pelo projeto até aqui.

A seguir listamos todas as atividades levantadas e planejadas, agrupadas de acordo com sua classificação de seus aspectos conforme definidos acima utilizando o seguinte padrão:




O tipo da atividade define se a sugestão para a execução da ação é **imediata** (*a ser executada pela parte responsável ainda dentro do prazo e escopo do projeto atual*) ou se é **contínua** (*a ser executada pelo DPO do controlador em etapas complementares/futuras de gestão do SGPD*).

## Aspectos operacionais e administrativos (23)

As atividades mais associadas aos aspectos operacionais e administrativos de adequação à LGPD que devem ser executadas para completar a adequação do Controlador dentro dos limites do projeto em questão são:

- **[Imediata] - Atualizar os dados dos DPOs dos operadores [ESP - SP]**
  - *Descrição*: Contatar os operadores, obter informações sobre o DPO (nome e contato) e atualizar o cadastro desses operadores no PCP.

- **[Imediata] - Ajustar a Política de Privacidade completa do controlador [ESB – SP]**
  - *Descrição*: Ajustar a Política de Privacidade completa do controlador, garantindo que o endereço do Portal do Titular (item 2) esteja correto, e que não haja indicação de e-mail como canal para falar com o DPO (item 6.8), visto que o canal é único, via Portal do Titular.

- **[Imediata] - Obter o aceite formal da Política de Privacidade [ESB – SP]**
  - *Descrição:* Obter o aceite formal da Política de Privacidade completa do controlador de todos os colaboradores internos da entidade, documentando o compromisso e aceite de todos em relação às regras ali definidas.

- **[Imediata] - Obter o aceite formal da Política de Cookies [ESB – SP]**
  - *Descrição:* Obter o aceite formal da Política de Cookies completa do controlador de todos os colaboradores internos da entidade, documentando o compromisso e aceite de todos em relação às regras ali definidas.

- **[Imediata] - Revisar a Política de Segurança do controlador [ESB - SP]**
  - *Descrição*: Garantir que a Política de Segurança do controlador, elaborada pela NEXT4IT, seja completa e atenda à LGPD e as melhores práticas de gestão de privacidade e segurança da informação.

- **[Imediata] - Atualizar a Política de Segurança para todas as medidas técnicas [ESB – SP]**
  - *Descrição*: Garantir que a Política de Segurança do controlador, elaborada pela NEXT4IT, preveja todas as medidas técnicas em uso pelo controlador, garantindo que o documento esteja atualizado, prevendo todas as medidas técnicas de segurança atualmente em uso no SGPD.

- **[Imediata] - Obter o aceite formal da Política de Segurança [ESB – SP]**
  - *Descrição*: Obter o aceite formal da Política de Segurança completa do controlador de todos os colaboradores internos da entidade, documentando o compromisso e aceite de todos em relação às regras ali definidas.

- **[Imediata] - Elaborar a Política de Descarte de Dados do controlador [Omnisblue]**
  - *Descrição*: Criar uma política que defina as regras de descarte de dados pessoais de acordo com as categorias de artefatos (documentos) utilizadas pelo controlador.

- **[Imediata] - Elaborar a Política de Mesa Limpa do controlador [Omnisblue]**
  - *Descrição*: Criar uma política que estabeleças as melhores práticas de "mesa limpa" para uso no dia a dia do controlador.

- **[Imediata] - Implantar o processo de Gestão de Riscos, Incidentes e Notificações [Omnisblue]**
  - *Descrição:* Implantar o processo de Gestão de Riscos, Incidentes e Notificações no controlador, com apoio do Privacy & Compliance Project (PCP) e do Privacy Action (PAC), treinando os usuários do controlador na operação do processo.

- **[Imediata] - Implantar o processo de Emissão do DPIA / LIA [Omnisblue]**
  - *Descrição*: Implantar o processo de Emissão do DPIA / LIA no controlador, com apoio do Privacy Action (PAC), treinando os usuários do controlador na operação do processo.

- **[Imediata] - Implantar o processo de Gestão de Consentimentos [Omnisblue]**
  - *Descrição*: Implantar o processo de Gestão de Consentimentos no controlador, com apoio do Privacy Action (PAC), treinando os usuários do controlador na operação do processo.

- **[Imediata] - Implantar o processo de Gestão de Políticas [Omnisblue]**
  - *Descrição*: Implantar o processo de Gestão de Políticas no controlador, com apoio das ferramentas disponibilizadas, treinando os usuários do controlador na operação do processo.

- **[Imediata] - Implantar o processo de Gestão e Avaliação de Terceiros [Omnisblue]**
  - *Descrição:* Implantar o processo de Gestão e Avaliação de Terceiros no controlador, com apoio do Due Diligence Portal (DDP), treinando os usuários do controlador na operação do processo.

- **[Imediata] - Inventariar o processo de Gestão e Avaliação de Terceiros no Privacy & Compliance Project (PCP) [Omnisblue]**
  - *Descrição*: Inventariar o processo de Gestão e Avaliação de Terceiros no Privacy & Compliance Project (PCP), garantindo que seus ativos, artefatos, metadados e finalidades foram inventariados e estão disponíveis para consulta.

- **[Imediata] - Emitir o DPIA / LIA pré-adequação do controlador [Omnisblue]**
  - *Descrição:* Emitir um DPIA e um LIA completo para registrar o status atual do SGPD, mesmo antes de completar o ciclo de adequação do controlador.

- **[Contínua] - Implementar a Política de Descarte de Dados [ESB – SP]**
  - *Descrição:* Implementar a Política de Descarte de Dados nas finalidades associadas e indicar os processos de descartes de cada finalidade em seu respectivo inventário, garantindo que o controlador não mais armazenará dados pessoais por tempo além do necessário para cumprimento da finalidade.

- **[Contínua] - Monitorar o uso dos dados pessoais pelo legítimo interesse do controlador [ESB – SP]**
  - *Descrição:* Monitorar o uso dos dados pessoais pelo legítimo interesse e emitir o LIA associado a esses tratamentos sempre que necessário.

- **[Imediata] - Indicar o processo de gestão do consentimento nas finalidades inventariadas [Omnisblue]**
  - *Descrição:* Atualizar os dados das finalidades que usam o consentimento como base legal indicando o prazo de validade desses consentimentos e os processos de obtenção desses consentimentos, dando segurança ao controlador que ele pode gerenciar esses consentimentos de acordo com o que estabelece a LGPD.

- **[Imediata] - Inventariar os contratos de operadores [ESB – SP]**
  - *Descrição*: Inventariar os contratos associados aos tratamentos de dados realizados pelos operadores e indicar a associação entre esses contratos, os operadores e suas respectivas finalidades de tratamento de dados.

- **[Imediata] - Implementar requisitos de uso de dispositivos pessoais em ambiente de trabalho [ESB-SP]**
  - Descrição: Fazendo uso da nova política de segurança da informação do controlador, apresentar aos colaboradores da unidade/departamento as regras a serem seguidas para o uso de dispositivos pessoais em ambiente de trabalho, e conscientizar os colaboradores sobre a obrigatoriedade de aderência à essas diretrizes, sob pena de sanções administrativas.

- **[Imediata] - Implementar política de mesa limpa na unidade/departamento [ESB-SP]**

  - *Descrição*: Fazendo uso da nova política de segurança do controlador, apresentar as regras de "mesa limpa" que devem ser observadas na unidade/departamento, garantindo segurança e disponibilidade ideal das informações físicas tratadas na área.
    Essas regras devem ser demonstradas aos colaboradores, bem como a obrigatoriedade de serem seguidas, sob pena de sanções administrativas.

- **[Imediata] - Implementar política de impressão na unidade/departamento [ESB – SP]**
  - *Descrição*: Fazendo uso da nova política de segurança do controlador, apresentar as regras de "compartilhamento de impressão" de que devem ser observadas na unidade/departamento, garantindo segurança e disponibilidade ideal das informações físicas tratadas na área.
    Essas regras devem ser demonstradas aos colaboradores, bem como a obrigatoriedade de serem seguidas, sob pena de sanções administrativas.

## Aspectos tecnológicos (15)

As atividades mais associadas aos aspectos técnicos e tecnológicos de adequação à LGPD que devem ser executadas para completar a adequação do Controlador dentro dos limites do projeto em questão são:

- **[Imediata] – Ajustar a publicação da Política de Privacidade no website corporativo [ESB – SP]**
  - *Descrição*: Ajustar a publicação da Política de Privacidade completa do controlador na área de LGPD do website corporativo do controlador, garantindo que o endereço do Portal do Titular (item 2) esteja correto, e que não haja indicação de e-mail como canal para falar com o DPO (item 6.8), visto que o canal é único, via Portal do Titular.

- **[Imediata] - Publicar a Política de cookies no website corporativo [ESB – SP]**
  - *Descrição*: Publicar a Política de cookies completa do controlador na área de LGPD do website corporativo do controlador, garantindo que as regras de uso de cookies no website corporativo do controlador estejam disponíveis a todos, dando maior transparência na gestão do SGPD. Atualmente a política de cookies publicada é a da Omnisblue.

- **[Imediata] - Enviar todos os pedidos de consentimento aos titulares de dados [ESB – SP]**
  - *Descrição*: Configurar o Privacy Action (PAC) e enviar todos os pedidos de consentimento aos titulares de dados, garantindo que os consentimentos sejam obtidos e guardados para eventual consulta e revogação.

- **[Imediata] - Disponibilizar o Due Diligence Portal (DDP) em ambiente de produção [Omnisblue]**
  - *Descrição*: Implementar o Due Diligence Portal (DDP) em ambiente de produção e realizar o treinamento com o time do controlador, garantindo que o módulo possa ser utilizado em ambiente real de negócio.

- **[Contínua] - Implementar as medidas técnicas de CONFIDENCIALIDADE [ESB – SP]**
  - *Descrição*: Implementar as medidas técnicas de CONFIDENCIALIDADE sugeridas para cada ativo, melhorando o índice de confiabilidade desses ativos

- **[Contínua] - Implementar as medidas técnicas de INTEGRIDADE [ESB – SP]**
  - *Descrição*: Implementar as medidas técnicas de INTEGRIDADE sugeridas para cada ativo, melhorando o índice de confiabilidade desses ativos

- **[Contínua] - Implementar as medidas técnicas de DISPONIBILIDADE [ESB – SP]**
  - *Descrição*: Implementar as medidas técnicas de DISPONIBILIDADE sugeridas para cada ativo, melhorando o índice de confiabilidade desses ativos

- **[Contínua] - Implementar política de "senha forte" nos ativos eletrônicos utilizados na unidade/departamento [ESB-SP]**
  - *Descrição*: O acesso aos ativos de informação eletrônicos utilizados na unidade/departamento deve ocorrer mediante o uso de "senhas fortes", compostas por letras, números e caracteres especiais. Além disso, a partir do primeiro acesso do usuário, esses ativos devem forçar a troca das senhas-padrão, garantindo assim que cada usuário seja responsável por definir sua senha forte.

- **[Imediata] - Implementar bloqueio automático de telas por inatividade nos dispositivos corporativos [ESB-SP]**
  - *Descrição*: Os dispositivos utilizados para acessar os ativos de informação eletrônicos em uso na unidade/departamento (desktops e notebooks) devem ser configurados de forma que eles realizem o travamento da tela de forma automática quando da inatividade do usuário após 5 (cinco) minutos.

- **[Contínua] - Implementar segregação de acesso de discos nos dispositivos corporativos [ESB-SP]**
  - *Descrição*: Os dispositivos utilizados para acessar os ativos de informação eletrônicos em uso na unidade/departamento (desktops e notebooks) devem ser configurados de forma que o acesso a eles, realizado mediante usuário e senha pessoal, segregue discos, partições e pastas, garantindo que cada usuário tenha acesso apenas às suas informações.

- **[Contínua] - Implementar criptografia de discos nos dispositivos corporativos [ESB-SP]**
  - *Descrição*: Os dispositivos utilizados para acessar os ativos de informação eletrônicos em uso na unidade/departamento (desktops e notebooks) devem ser configurados de forma que seus discos possuam criptografia ativada, garantindo que apenas usuários com senhas possam acessar o conteúdo de seus discos.
    Para equipamentos Windows, utilizar, por exemplo, o BitLocker.

- **[Imediata] - Implementar medidas técnicas de segurança contra vírus e malware nos dispositivos pessoais [ESB-SP]**
  - *Descrição*: Os dispositivos pessoais dos colaboradores da unidade/departamento, utilizados para a realização de atividades de trabalho, devem estar configurados com as medidas técnicas de segurança previstas na política de segurança do controlador, garantindo que eles possam se conectar ao ambiente tecnológico do controlador mitigando riscos de compartilhamento de vírus e malware.

- **[Contínua] - Implementar medidas técnicas de criptografia nos dispositivos pessoais [ESB-SP]**
  - *Descrição*: Os dispositivos pessoais dos colaboradores da unidade/departamento, utilizados para a realização de atividades de trabalho, devem estar configurados com as medidas técnicas de criptografia, garantindo que acessos indevidos não realizem o compartilhamento de dados pessoais com pessoas não autorizadas.

- **[Contínua] - Implementar procedimento de backup/limpeza de disco em dispositivos corporativos da unidade/departamento [ESB-SP]**
  - *Descrição*: Dispositivos corporativos (desktops e notebooks) devem passar por atividades de limpeza de disco antes de serem enviados para manutenção ou serem transferidos de responsável, garantindo assim que dados pessoais ali armazenados não sejam acessados por terceiros sem a devida autorização.

- **[Contínua] - Implementar monitoramento de câmeras nos ambientes onde são armazenados os ativos físicos [ESB-SP]**
  - *Descrição*: Os documentos (artefatos) físicos em uso na unidade/departamento devem ser armazenados em local seguro, com monitoramento de câmera que garanta a possibilidade de se consultar histórico de acesso ao local.
    Sugere-se que as imagens sejam armazenadas por um período de ao menos 30 (trinta) dias, e descartadas/substituídas após esse período.

## Aspectos jurídicos (02)

As atividades mais associadas aos aspectos jurídicos de adequação à LGPD que devem ser executadas para completar a adequação do Controlador dentro dos limites do projeto em questão são:

- **[Imediata] - Apostilar / aditivar os contratos atualmente vigentes [ESB – SP]**
  - *Descrição*: Apostilar / aditivar os contratos atualmente vigentes com as novas cláusulas contratuais que endereçam os temas de privacidade e segurança da informação (contratos com titulares, operadores e fornecedores).

- **[Imediata] - Inventariar todos os contratos com operadores [ESB – SP]**
  - *Descrição:* Levantar e inventariar todos os contratos com operadores e associá-los às suas respectivas finalidades de tratamento de dados no Privacy & Compliance Project (PCP), garantindo que todas as finalidades inventariadas e indicadas como que fazem uso de operadores terão contratos inventariados e associados aos seus respectivos operadores no PCP.

## Aspectos evolutivos (02)

Adicionalmente às ações prevista acima, que tratam exclusivamente do escopo do projeto atual, durante a etapa de **Preparação** detectamos alguns riscos adicionais que endereçam um futuro aumento da abrangência do escopo de adequação à LGPD por parte do Controlador. Esses riscos geram as seguintes sugestões:

- **[Contínua] - Expandir a abrangência do SGPD [ESB - SP]**
  - *Resultado esperado*: Expandir a abrangência do SGPD para as demais áreas de negócio do controlador, garantindo que todas as áreas de negócio do controlador estarão cobertas pelo escopo de adequação à LGPD.

- **[Contínua] - Realizar a modelagem dos processos de negócio [ESB - SP]**
  - *Resultado esperado*: Realizar a modelagem dos processos de negócio em BPMN (ou outra notação) e associar os diagramas a cada um dos processos inventariados.

## Conclusão

As ações sugeridas neste Plano de Ação já foram cadastradas no PCP para controle e acompanhamento de seus resultados, e este documento deve ser conhecido por todos os stakeholders do Controlador que porventura sejam envolvidos direta ou indiretamente na execução dessas ações.

Os prazos, as datas planejadas para a execução de cada atividade prevista neste Plano de Ação e eventuais interdependências entre as atividades são aspectos que estão detalhados no *Cronograma do projeto* que deve ser atualizado considerando os detalhes aqui definidos.
Todas as atividades foram também cadastradas no PCP para acompanhamento eletrônico do avanço de suas tratativas.

As atividades de adequação definidas neste plano que forem de responsabilidade da Omnisblue, de acordo com o escopo dos serviços contratados, serão realizadas de acordo com Plano do Projeto e serão acompanhadas pela ESB - SP.
Para as ações de responsabilidade da ESB - SP, a Omnisblue se coloca à disposição para apoio remoto e maiores esclarecimentos, durante um período de até 30 (trinta) dias após o término da última atividade técnica a ser executada pelo time da Omnisblue tal como definido neste documento, em observância aos princípios de boa-fé e parceria já estabelecidos entre as partes.