omnisblue

# GUIA DE PREMISSAS E PADRÕES DE DESENVOLVIMENTO DE SOFTWARE

**Omnisblue**

## 1. OBJETIVO DO DOCUMENTO

Neste guia iremos estabelecer os critérios mínimos de qualidade, as premissas e restrições que todas as equipes de desenvolvimento de software (interna ou externa) a serviço da Omnisblue devem seguir durante a execução de projetos de desenvolvimento de produto de Tecnologia da Informação (softwares, sistemas, aplicativos etc.).

Este documento está associado à nossa **Política de Governança Corporativa** e reforça nosso compromisso com qualidade e nossa busca por excelência na prestação de nossos serviços.

As regras aqui definidas se aplicam a todos os desenvolvimentos de softwares executados pela Omnisblue, estejam eles relacionados a produtos a serem comercializados no mercado que atuamos ou mesmo para produtos de uso interno na nossa empresa.

Os padrões aqui definidos devem também ser observados por fornecedores terceirizados que porventura nossa empresa venha a fazer uso, e, nesse caso, este documento deve ser compartilhado com esses fornecedores antes de eventuais projetos com esses terceiros serem iniciados.

## 2. Sobre nossa engenharia de software

Nós na Omnisblue entendemos que o desenvolvimento de soluções de tecnologia da informação, em especial softwares, é uma atividade complexa e de alto teor intelectual, que, acima de tudo, envolve uma série de disciplinas interligadas que devem trabalhar de forma harmônica em busca de alguns objetivos comuns e atendendo a alguns princípios básicos:

- Uma solução deve sempre resolver um ou mais problemas: Só há necessidade de se criar softwares que resolvam problemas conhecidos;
- Projetos de TI devem apresentar resultados de soma positiva: A criação de soluções tecnológicas deve agregar valor observável a todos os envolvidos;
- Maximização de resultados de negócio: A TI (e seus produtos) deve sempre ser compreendida como ferramentas de apoio a objetivos maiores do negócio que ela apoia, e não deve ser gerenciada como uma atividade finalística;
- Tecnologia é ferramenta, e apenas isso: A escolha por tecnologias específicas jamais deve superar os objetivos a serem alcançados pelo projeto. Uma determinada linguagem de programação, uma tecnologia de Banco de Dados ou uma determinada arquitetura deve ser sempre tratadas como ferramentas, e nada além disso. As escolhas tecnológicas e arquiteturais devem ser feitas a partir do entendimento das necessidades de negócio que cada projeto busca atender, e nada além disso.

A partir da compreensão dessas regras básicas, a Omnisblue elaborou uma metodologia de desenvolvimento de produtos e serviços e, a partir dessa metodologia, nasce o **Processo de Engenharia de Software da Omnisblue**, que deve ser seguido sempre que um projeto executado pela nossa empresa gere um software.

O Processo de Engenharia de Software da Omnisblue é composto pelas seguintes etapas e seus respectivos entregáveis:

**Etapa de Análise**: Trata-se da etapa onde devemos entender o problema a ser resolvido pelo futuro software e estabelecer os requisitos funcionais e não funcionais que a solução deverá atender.

*Entregáveis:* Modelagem de processos de negócio em BPMN 2.0 (para os processos atuais e para os processos atualizados após implantação do software), especificação funcional detalhando os requisitos e regras de negócio que o software deve atender, protótipo navegável da solução a ser desenvolvida.

**Etapa de Design**: É onde os requisitos detalhados na Etapa de Análise serão agora transformados em especificações técnicas e de componentes, e a arquitetura tecnológica e a especificação da infraestrutura que irá suportar a futura aplicação é desenhada.

*Entregáveis*: Modelagem de entidade-relacionamento das tabelas (MER), especificação de arquitetura e especificação de infraestrutura.

**Etapa de Implementação:** Etapa onde o software é codificado e testado, tanto em ambiente de desenvolvimento ou homologação.

*Entregáveis:* Código-fonte do software e seus componentes e bibliotecas, casos de teste, relatórios de deployment e relatórios de teste.

**Etapa de Implantação**: Entrega do software em ambiente de produção, para uso real dos usuários finais, e preparação desses usuários para fazer uso da nova aplicação.

*Entregáveis:* Ambiente de produção configurado e pronto para uso, plano de treinamento, relatório de treinamentos, manuais de uso do software.

Estabelece-se que todas as etapas acima detalhadas devem ser executadas em todos os projetos de produção de software da Omnisblue. Para casos de exceção, os líderes e gestores de cada projeto devem justificar qualquer alteração no processo, considerando sempre que essas alterações não devem, em nenhuma hipótese, serem incompatíveis com as premissas estabelecidas no início desta seção.
Os detalhes de cada entregável (e seus respectivos modelos) e cada etapa devem ser obtidos nas documentações auxiliares do **Processo de Engenharia de Software da Omnisblue**, disponibilizadas no nosso portal corporativo.

## 3. Sobre os ambientes utilizados durante o desenvolvimento de software

Todo projeto de desenvolvimento de software na Omnisblue fará uso de mais de um ambiente onde a solução será disponibilizada, a depender da etapa do ciclo de desenvolvimento que o projeto se encontra e das atividades em execução.
Esses ambientes devem ser gerenciados e acessados apenas pelos papéis associados a eles, de acordo com a necessidade de uso de cada ambiente.
Estabelece-se que, no mínimo, cada desenvolvimento de software deve fazer uso dos seguintes ambientes:

**Ambiente de desenvolvimento:** Ambiente onde o desenvolvimento (codificação) do software é realizado. Esse ambiente compreende servidores de aplicação e banco de dados que poderão ser disponibilizados em ambiente interno (*on-premises*) ou externo (cloud), os repositórios de código-fonte centralizado da Omnisblue e as IDEs e repositórios locais de código-fonte disponibilizados nas estações de trabalho dos desenvolvedores ou arquitetos associados ao projeto. Esse ambiente é de uso exclusivo da equipe da Omnisblue, e o cliente não deve ter acesso a nenhum componente associado a ele.

**Ambiente de homologação**: Ambiente onde são disponibilizadas as versões intermediárias dos softwares em desenvolvimento. Esse ambiente compreende servidores de aplicação e banco de dados que poderão ser disponibilizados em ambiente interno (*on-premises*) ou externo (cloud), e os repositórios de código-fonte centralizado da Omnisblue. A atualização desses ambientes deve ser sempre realizada por administradores e, quando houver necessidade de atualização da base de dados, isso deve ser registrado para eventuais auditorias. Esse ambiente pode ser utilizado tanto pela equipe Omnisblue para testes e homologações, como por usuários do cliente para atividades de capacitação e homologação.

**Ambiente de produção:** Ambiente onde são disponibilizadas as versões finais dos softwares prontos. Esse ambiente compreende servidores de aplicação e banco de dados que poderão ser disponibilizados em ambiente interno (*on-premises*) ou externo (cloud), e eventuais clients necessários para o uso do software. A atualização desses ambientes deve ser sempre realizada por administradores e, quando houver necessidade de atualização da base de dados, isso deve ser registrado para eventuais auditorias, desde que essa atualização não viole nenhuma regra de segurança (veja a seguir). Esse ambiente só pode ser utilizado por usuários do cliente, e eventualmente por colaboradores da Omnisblue para atividades de suporte, respeitando as definições contratuais estabelecidas entre a empresa e seu cliente.

Cabe à gestão de cada projeto de desenvolvimento de software definir a necessidade de ambientes adicionais aos aqui detalhados, de acordo com os objetivos e especificidades de cada projeto.
O acesso a esses ambientes deve ser gerenciado e controlado, por perfil, garantindo níveis de confidencialidade adequados a cada projeto.
Todo o acesso de configuração e deployment dos ambientes de homologação e produção deve ser logado.

## 4. Padrões de segurança

O desenvolvimento dos softwares deve atender, além das definições já expostas anteriormente, a critérios técnicos e funcionais que visem maximizar os níveis de confiabilidade da informação gerenciada por cada software.

O nível de confiabilidade da informação é composto pelos parâmetros de confidencialidade, integridade e disponibilidade da informação que é processada por cada produto.
Para saber mais sobre o nível de confiabilidade de informação e como a Omnisblue trata sobre o tema, consulte nossa **Política de Segurança da Informação.**

De qualquer maneira, toda atividade de produção de software deve atentar para boas práticas de segurança, seja na definição e manutenção da arquitetura, seja na codificação de cada componente do software em desenvolvimento.
As práticas a seguir devem ser observadas em todos os projetos de desenvolvimento de software da Omnisblue, e qualquer exceção deve ser previamente discutida, justificada e aprovada formalmente pela gestão do projeto e pelas lideranças da empresa.

**Codificação Segura:** Os códigos-fontes produzidos durante o ciclo de desenvolvimento de um software (tanto para a criação de um novo produto, como para a manutenção de um produto já existente), devem obedecer às seguintes premissas:

- Valide as entradas de dados da aplicação garantindo que não seja permitido inclusão de código Javascript em seus campos, evitando assim ataques Cross-Site Scripting (XSS);
- Use o cabeçalho de segurança x-xss-security para aplicações web;
- Filtre e valide parâmetros no servidor na chegada das requisições para rejeitá-la ou eliminar o risco de SQL Injection;
- Troque os caracteres-chave por entidades HTML, de forma que o conteúdo da variável seja sempre considerado texto e nunca uma tag ou parte de um script;
- Não permita que as páginas administrativas sejam indexadas nos mecanismos de buscas;
- Não exiba na tela mensagens de exceções vindas diretamente do banco de dados;
- Gerencie as exceções de segurança que forem lançadas na aplicação, para que se possa ter conhecimento dos ataques que estão sendo feitos contra sua aplicação;
- Não inclua senhas ou chaves no código-fonte;
- Grave as senhas de usuário no banco de dados utilizando um algoritmo de hashing;
- Utilize sempre protocolo HTTPS para aplicações web;
- Nunca use cookies para armazenar informações altamente sensíveis ou críticas. Por exemplo: não use cookies para lembrar as senhas dos usuários;
- Estabeleça uma política para criação de logs das principais rotinas de processamento de dados do software em desenvolvimento e crie os mecanismos de log e os implemente nessas rotinas.

**Controle de Acesso e Autenticação:** As informações tratadas pelos softwares desenvolvidos pela Omnisblue devem ter seu acesso gerenciado, atendendo às seguintes premissas:

- Valide sempre as permissões do usuário ao acessar uma funcionalidade, restringindo o acesso tanto aos dados quanto aos recursos implementados;
- Utilize o conceito de privilégio mínimo para execução dos processos da aplicação, ou seja, o mínimo de permissões para que seja efetuado o serviço;
- Controle a quantidade de tentativas de login e bloquear, caso necessário;
- Recomende ao usuário a confecção de senhas fortes, determinar restrições de quão fortes as senhas estão;
- Utilize o CAPTCHA em formulários, principalmente em autenticações;
- Altere o algoritmo de autenticação de forma a recuperar somente a senha do usuário e depois compará-la com a senha recebida como parâmetro;
- Não utilize a senha de administrador para acessar o banco de dados;
- Quando possível, implemente a autenticação de dois fatores.

**Proteção de Dados:** Os softwares produzidos pela Omnisblue, em essência, irão realizar o tratamento de dados (pessoais ou não). A proteção desses dados é nossa responsabilidade, portanto:

- Evite guardar em campos ocultos informações críticas ao funcionamento da aplicação, que o usuário não poderia modificar normalmente, como identificadores, preços e status;
- Caso o uso de campos ocultos seja realmente necessário, faça uma validação que os verifique tão logo a requisição chegar ao servidor;
- Valide as informações de todos os campos de um formulário também no servidor (backend), inclusive o tamanho dos campos, independentemente de existir ou não uma validação no frontend utilizando Javascript;
- Não utilize Javascript para implementar regras de negócio importantes e essenciais para segurança. Se for realmente necessário, lembre-se de replicar a lógica e validar as informações no servidor (backend);
- Tenha atenção ao permitir o upload de arquivos, valide o formato e tamanho dele. E jamais exiba o caminho onde a imagem foi salva;
- Armazene todos os arquivos de configuração e sigilosos (extensões: .cfg, .ini, .conf, .log, .pdf, .gbd ) em uma pasta inacessível pela web e gerencie com rigor o acesso aos dados sigilosos, quando for necessário disponibilizá-los.

**Testes de Segurança:** Toda aplicação desenvolvida pela Omnisblue para oferta ao mercado e clientes externos deve passar por rotinas formais de teste de segurança antes de serem ofertadas no mercado e colocadas à disposição de nossos clientes. Essas rotinas de testes e auditorias de segurança devem ser realizadas por empresa parceira externa, devidamente capacitada e com experiência comprovada no tema. O resultado dessas rotinas de auditorias poderá endereçar mudanças arquiteturais nos softwares desenvolvidos e em desenvolvimento e, quando isso ocorrer, caberá à gestão e à liderança da empresa priorizar as eventuais mudanças endereçadas.

## 5. Disposições gerais

A Omnisblue é responsável pela elaboração, supervisão e manutenção deste Guia de premissas e padrões de desenvolvimento de software, que é parte integrante tanto de seu Sistema de Gerenciamento de Privacidade e Proteção de Dados (SGPD) como de sua metodologia de desenvolvimento de produtos e serviços.

O teor deste guia poderá ser atualizado ou modificado a qualquer momento, conforme a finalidade ou conveniência da Omnisblue, cabendo aos colaboradores e parceiros da empresa verificá-lo sempre com seus gestores e líderes.

Ocorrendo atualizações neste documento, a Omnisblue notificará aos colaboradores e parceiros mediante as ferramentas de gestão interna. Os colaboradores e parceiros estarão vinculados aos novos termos deste documento a partir da entrega da notificação sobre as atualizações.

Quando a Omnisblue fizer uso de terceiros para o desenvolvimento de softwares (de forma total ou parcial), esse terceiro deverá respeitar as condições aqui estipuladas, bem como todas as definições do Sistema de Gerenciamento de Privacidade e Proteção de Dados (SGPD) em vigor na Omnisblue, obrigatoriamente. Esse compromisso é documentado em cláusulas contratuais definidas nos contratos firmados entre a Omnisblue e nossos fornecedores.

**Versão: 1.2**

**Data de início de vigência: 06 de março de 2023**