omnisblue

LGPD | COMPLIANCE

GUIA DE MEDIDAS TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO

A Omnisblue define, em seu Manual de Segurança da Informação, nossas diretrizes que devem ser observadas ao tratarmos do tópico “Segurança da Informação”.

Este guia, anexo ao Manual de Segurança da Informação, orienta e estabelece as diretrizes corporativas técnicas da Omnisblue para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprido e aplicada em todas as áreas da empresa.

As definições aqui dispostas estão baseadas em recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como melhores práticas de mercado e como fruto do aprendizado que obtivemos ao longo do tempo na gestão de nossos ativos e da segurança que os permeia.

Nos preocupamos também em garantir que este documento está em conformidade com as legislações vigentes do nosso país que trata, direta ou indiretamente, sobre o tema, tal como a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/18).

Nota de confidencialidade: Por detalhar nossas estratégias e definir as medidas técnicas de segurança que a Omnisblue implementa, este documento não deve ser compartilhado com terceiros, sob risco de expormos informações que poderão ser utilizadas de forma maliciosa contra nossas defesas e proteções e, portanto, endereçar riscos de segurança por si só.

omnisblue

LGPD | COMPLIANCE

Sumário

1. Glossário

1.1. Para os fins deste documento, devem ser consideradas as seguintes definições e descrições para seu melhor entendimento:

I. **Artefato:** São as fichas, documentos ou cadastros que aglutinam um ou mais Dado ou Dado Pessoal. Exemplo: O cadastro dos clientes da Omnisblue é um artefato que abriga, entre outros, o nome e o e-mail (dados pessoais) de seus clientes;

II. **Ataque:** evento de exploração de vulnerabilidades. Ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

III. **Ativos da Informação:** entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e/ou excluir uma informação. No contexto deste documento, entende-se por ativos de informação os ativos eletrônicos (sistemas e produtos de tecnologia) e os ativos físicos (documentos físicos, pastas etc.) que gerenciam artefatos (documentos) que possuem dados e dados pessoais tratados pela Omnisblue;

IV. **Backup:** cópia de segurança de dados em mídia magnética (disco ou fita) ou em nuvem que pode ser restaurada pelo processo conhecido como “restore” em caso da perda dos dados originais;

V. **Confiabilidade:** Trata-se do nível de segurança total atribuído a um determinado ativo de informação, e é a soma dos níveis de Confidencialidade, Integridade e Disponibilidade da informação atribuídos a esse ativo;

VI. **Confidencialidade:** Trata-se do nível de sigilo de informação que um determinado ativo de informação consegue garantir. É a propriedade do ativo que garante que a informação tratada pelo ativo não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados;

VII. **Criptografia:** mecanismo de segurança e privacidade que torna determinada comunicação ou dados indecifráveis para quem não tem acesso aos códigos de “tradução”. A criptografia auxilia na proteção de todos os conteúdos armazenados ou transmitidos entre duas ou mais fontes, evitando a interceptação por terceiros;

VIII. **Crise:** um evento ou série de eventos de grande dimensão que possam trazer danos à imagem da organização ou prejudicar seu relacionamento com clientes, acionistas, órgãos reguladores, investidores e demais partes interessadas, podendo ou não acarretar perdas financeiras para a Omnisblue;

IX. **Dados Pessoais:** significam as informações relacionadas à pessoa natural identificada ou identificável;

X. **Dados Pessoais Sensíveis:** significam as informações relacionadas à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a uma pessoa natural;

XI. **Disponibilidade:** Trata-se do nível de prontidão que que um determinado ativo de informação consegue garantir para apresentar uma determinada informação a alguém. É a propriedade do ativo que garante que a informação tratada pelo ativo pode ser acessível e utilizável sob demanda, pois garante que os ativos (e os dados) estão funcionando (disponíveis) quando necessário;

XII. **Guia de Gerenciamento das Políticas de Segurança da Informação:** documento interno da Omnisblue que define as regras do ciclo de vida das deste documento e do Manual de Segurança da Informação;

XIII. **Informação:** resultante do processamento, manipulação e organização de dados, constitui uma mensagem sobre um determinado assunto, fenômeno ou evento;

XIV. **Integridade:** Trata-se do nível de exatidão da informação disponibilizada por um determinado ativo de informação. É a propriedade do ativo que garante que a informação tratada pelo ativo é correta e consistente com o esperado, e busca assegurar que sejam prevenidas modificações não autorizadas em dados tratados no ativo;

XV. **LGPD:** Trata-se da Lei Geral de Proteção de Dados, Lei nº 13.709/2018;

XVI. **Leis Aplicáveis:** significa todas as leis, regras, regulamentos, ordens, decretos, orientações normativas e autorregulamentações aplicáveis à proteção de dados, incluindo, sem limitação, a proteção de dados pessoais no Brasil e fora do País.

XVII. **Log:** processo de registro de eventos relevantes num sistema computacional;

XVIII. **Manual de Segurança da Informação:** documento interno da Omnisblue que define as diretrizes de segurança da informação a serem observadas na operação da empresa;

XIX. **Política de Classificação da Informação:** documento interno da Omnisblue que determina as regras de classificação das informações tratadas pela empresa e como o uso desses dados deve ser governando de acordo com a criticidade associada a eles;

XX. **Política de Descarte de Dados:** documento interno da Omnisblue que determina regras de descarte de dados pessoais e definições de algumas medidas operacionais de segurança adicionais a este guia;

XXI. **Política de Gestão de Mudanças:** documento interno da Omnisblue que define as regras de como as mudanças organizacionais, funcionais, tecnológicas e de relacionamento com parceiros devem ser controladas e gerenciadas;

XXII. **Política de Segurança em Estações de Trabalho e Recursos de Computação Móvel:** documento interno da Omnisblue que estabelece as diretrizes para o uso de recursos individuais (estações de trabalho) e ambientes de trabalho em nuvem dentro da empresa, e suas respectivas regras de segurança;

XXIII. **Risco:** o risco mensura a probabilidade e o impacto de possíveis resultados negativos associados a incidentes que podem comprometer a confidencialidade, integridade e disponibilidade de dados ou ativos da informação;

XXIV. **Titulares dos Dados:** significam as pessoas físicas a quem se referem os Dados Pessoais que são objeto de Tratamento, nos termos do presente instrumento;

XXV. **Tratamento de Dados:** significa toda operação realizada com Dados e Dados Pessoais, incluindo a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XXVI. **Vazamento de dados:** qualquer quebra de sigilo ou disseminação de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

XXVII. **Violação de privacidade:** qualquer violação à legislação aplicável ou conduta e evento que resulte na ofensa privacidade do titular de dados, podendo tal ofensa ser originária da destruição acidental ou ilícita dos dados,

bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;

XXVIII. **Vírus:** programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

2. Diretrizes corporativas

2.1. A Omnisblue entende suas responsabilidades em relação aos dados e informações em tratamento pelo nosso time e, portanto, possui uma unidade específica de Segurança da Informação, compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da empresa.

2.2. Nosso Manual de Segurança da Informação estabelece nossas diretrizes de segurança que devem ser mantidas, adicionalmente, com as medidas técnicas detalhadas a seguir.

2.3. Conjuntamente às medidas técnicas que detalhamos neste documento, consideramos a privacidade dos Titulares de Dados envolvidos em nossas atividades como uma de nossas prioridades, e, portanto, a implementação dessas medidas deve ser sempre pautada pelo padrão privacy by design, que estabelece 7 (sete) princípios valiosos que devemos nos ater para garantir que a segurança da informação tem como objetivo final garantir a privacidade das pessoas desde a concepção de nossas estratégias, produtos e serviços. São eles:

2.3.1. **Prevenir antes de remediar:** devemos agir proativamente e gerenciar riscos para mitigar a probabilidade de ocorrência de incidentes;

2.3.2. **Privacidade como padrão (privacy by default):** dão devemos exigir nenhuma ação dos titulares de dados para que a privacidade de nossos produtos, serviços ou soluções seja “ativada”. A privacidade é o padrão;

2.3.3. **Privacidade incorporada ao projeto:** a privacidade não deve ser tratada como um componente adicional de nossos produtos, serviços ou soluções. Ela é algo intrínseco aos projetos;

2.3.4. **Soma positiva:** não devemos tratar a privacidade e questões de segurança da informação como uma formalidade apenas, isso tudo deve agregar valor aos nossos produtos ou serviços e não apenas ser uma obrigação;

2.3.5. **Segurança de ponta-a-ponta:** a proteção de dados deve ser algo presente desde o início das atividades de tratamento de dados realizados por nós, até quando os dados são destruídos;

2.3.6. **Visibilidade e transparência:** questões de privacidade e segurança da informação devem ser algo visíveis e transparentes para todos associados e participantes dos projetos, que devem saber as regras, práticas e tecnologias envolvidas nesses temas;

2.3.7. **Soluções centradas nos usuários finais:** entendemos que o maior interessado na privacidade é o Titular dos Dados e os donos das informações que manipulamos, logo, são os interesses desses que importam mais nas nossas decisões.

2.4. Transferência e Compartilhamento de Dados e Dados Pessoais com Terceiros:

2.4.1. A Omnisblue está comprometida em cumprir as regras e diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD) ao realizar transferências e compartilhamentos de dados pessoais com terceiros.

2.4.2. Abaixo, apresentamos as diretrizes que adotamos adota para garantir a proteção adequada dos dados e dados pessoais quando do compartilhamento dessas informações com terceiros:

I. **Base Legal para Transferência e Compartilhamento** – Devemos assegurar que todas as transferências e compartilhamentos de dados e dados pessoais com terceiros sejam baseados em bases legais. No caso de dados pessoais, devemos considerar as hipóteses previstas na LGPD, que incluem: (i) obter o consentimento do titular dos dados; (ii) cumprir com obrigações legais e regulatórias; (iii) proteger a vida ou a integridade física dos titulares; (iv) exercer direitos em processos judiciais ou nossos legítimos interesses ou de terceiros;

II. **Informação e transparência** - Antes de realizar a transferência ou compartilhamento de dados e dados pessoais, a Omnisblue fornece informações claras e transparentes aos proprietários desses dados. Essas informações incluem os detalhes sobre as finalidades da transferência, as categorias de dados envolvidos, a identificação dos terceiros envolvidos e as medidas de segurança adotadas para proteger as informações;

III. **Contrato ou Instrumento Similar** - A Omnisblue estabelece contratos ou instrumentos similares com os terceiros receptores dos dados e dados pessoais. Esses contratos contêm cláusulas que garantem a proteção adequada das informações transferidas. As cláusulas incluem medidas de segurança, confidencialidade, especificação das finalidades do tratamento, prazo de retenção dos dados, entre outros aspectos necessários para assegurar a conformidade com a LGPD e demais legislações;

IV. **Responsabilidade Solidária** – Reconhecemos nossa responsabilidade solidária pelos danos causados em caso de violação dos dados e dados pessoais pelos terceiros com os quais ocorreu a transferência ou compartilhamento. Assim, a empresa realiza uma avaliação criteriosa dos terceiros antes de compartilhar os dados e implementa medidas para garantir que eles cumpram as obrigações legais de proteção de dados;

V. **Transferências Internacionais** - No caso de transferências de dados pessoais para países fora do Brasil, a Omnisblue verifica se esses países oferecem um nível adequado de proteção de dados e dados pessoais. Caso contrário, a empresa adota medidas adicionais, como a utilização de cláusulas contratuais padrão, regras corporativas globais, selos, certificados ou códigos de conduta para garantir a proteção adequada dos dados pessoais transferidos.

3. Gestão de ativos de informação

3.1. Todos os ativos de informação utilizados pela Omnisblue devem ser conhecidos, inventariados, classificados e monitorados.

3.1.1. O uso desses ativos de informação é exclusivo para fins corporativos da empresa e, mesmo os ativos de uso pessoal (como estações de trabalho e seus periféricos) não podem ser transportados sem autorização prévia da gestão a qual o colaborador esteja hierarquicamente associado.

3.1.2. Quando for autorizado o transporte e de ativos de informação para outros locais diferentes dos de sua origem, esse transporte deve registrado e um Termo de Responsabilidade deve ser emitido para o colaborador que for executar a rotina;

3.2. Quando da devolução do ativo, o registro da movimentação deve ser atualizado com a data de devolução.

3.3. A classificação desses ativos está diretamente associada à classificação dos dados tratados nesse ativo, conforme definido na **Política de Classificação da Informação da Omnisblue**.

3.4. Os ativos de informação devem ser inventariados no **Lansweeper** para fins de gerenciamento de configuração e no **Privacy & Compliance Project (PCP)** para fins de governança de privacidade e adequação à LGPD.

3.5. Em ambos os sistemas de controle, cada ativo deve ter um responsável associado, que deve ser um colaborador interno da Omnisblue.

3.6. O status e nível de capacidade e disponibilidade de cada ativo da informação utilizado pela Omnisblue deve ser monitorado em tempo real através do uso da ferramenta **Zabixx**, que está configurada para gerar alertas de capacidade e disponibilidade aos administradores da infraestrutura da empresa.

3.7. Ativos da informação disponibilizados na plataforma Microsoft 365 devem ser configurados e monitorados fazendo uso do **Microsoft Defender e Microsoft Purview.**

3.8. Ativos da informação disponibilizados na Oracle Cloud Infrastructure (OCI) devem ser configurados e monitorados fazendo de ferramentas nativas da própria OCI/IaaS.

3.9. Todos os ativos de informação físicos e fornecidos por terceiros, em especial os servidores on-premises utilizados pela Omnisblue e/ou seus periféricos, devem sempre ser cobertos por contratos de suportes com os respectivos fabricantes, e esses contratos devem possuir Acordos de Níveis de Serviço compatíveis com as necessidades operacionais e comerciais da empresa e dos contratos estabelecidos com nossos clientes.

3.10. Gestão de redes de conectividade físicas e lógicas

3.10.1. A disponibilidade das redes físicas e lógicas utilizadas na Omnisblue devem atender, no mínimo, aos seguintes requisitos:

I. **Redes de internet:** Fazemos o uso de 2 (dois) links dedicados LAN-to-LAN que são gerenciados pelo firewall Fortigate e garantem alta disponibilidade de acesso seja de nossas estações de trabalho ou de nossos servidores de aplicação;

II. **Redes internas:** As instalações físicas da rede interna da Omnisblue são disponibilizadas sobre padrões mundiais de mercado quanto à qualidade de seus equipamentos e da sua estrutura e arquitetura;

III. Janelas de manutenção das redes de internet ou interna da Omnisblue devem seguir o procedimento de gestão de mudanças definido na **Política de Gestão de Mudanças da Omnisblue.**

3.10.2. As redes internas da Omnisblue são segregadas visando alcançar os seguintes objetivos:

I. **Minimizar o Impacto de Ataques:** Ao dividir a rede em segmentos, caso um segmento seja comprometido por um ataque, o impacto pode ser limitado àquele segmento específico. Isso impede que um ataque se propague facilmente por toda a infraestrutura da rede;

II. **Controle de Acesso:** A segregação permite um controle mais preciso sobre quem pode acessar quais recursos na rede. Isso é alcançado através da implementação de firewalls, políticas de acesso e outros mecanismos de controle;

III. **Proteção de Dados Sensíveis:** Ao isolar dados em segmentos específicos de acordo com sua classificação, podemos aplicar medidas de segurança mais rigorosas, como criptografia e controles de acesso mais restritos;

IV. **Mitigação de Ameaças Internas:** A segregação limita o acesso dos usuários a segmentos específicos necessários para suas funções. Isso reduz o potencial de danos causados por usuários mal-intencionados ou comprometidos internamente.

3.10.3. Nossa estrutura de rede está segmentada em 5 pilares principais:

I. **Rede de servidores internos:** Segmento de rede criado para hospedar os servidores on-premises da Omnisblue. Essa rede não tem nenhum tipo de comunicação externa;

II. **Rede de computadores dos colaboradores internos:** Segmento de rede criado para hospedar os computadores e notebooks dos colaboradores da Omnisblue;

III. **Rede VPN:** Segmento de rede criado para suportar colaboradores e fornecedores da Omnisblue que precisam se conectar à rede de servidores da empresa;

IV. **Rede Cloud:** Segmento de rede criado para suportar comunicação via VPN site-to-site com fornecedores/fabricantes de nuvem como Azure e OCI;

V. **Rede de computadores dos visitantes:** Segmento de rede criado para suportar computadores e dispositivos de visitantes da Omnisblue. Essa rede é completamente apartada e não tem nenhum tipo de comunicação com a rede de servidores internos e rede de computadores dos colaboradores internos.

4. Medidas técnicas de confidencialidade

4.1. Visando maximizar o nível de confidencialidade das informações tratadas pela Omnisblue, os ativos de informação utilizados na empresa para a execução de atividades internas ou para cumprimento de obrigações contratuais com terceiros devem ser configurados atendendo aos seguintes critérios de segurança:

4.1.1. Requisitos de qualidade e acesso físico aos ativos

I. O acesso às instalações físicas da Omnisblue só será permitido através da identificação pessoal de cada colaborador ou parceiro externo;

II. A Omnisblue sempre terá instalações físicas dispostas em edifícios que realizem o controle de acesso via catraca com identificação pessoal e intransferível de visitantes e seus colaboradores;

III. Para acessar as instalações físicas da Omnisblue é necessária a identificação prévia e uso de cartão individual para liberação nas catracas;

IV. As salas de servidores da Omnisblue só podem ser acessadas por pessoal autorizado, e esse controle é realizado através de fechadura eletrônica aberta por cartões individuais e intransferíveis emitidos aos técnicos responsáveis pela manutenção dos equipamentos;

V. As salas de servidores da Omnisblue contam com Sistemas de Detecção de Incêndio e Supressão e piso elevado;

VI. Todo o cabeamento físico de rede da Omnisblue é disponibilizado com cabos CAT-6;

VII. As estações de trabalho, além de terem seu acesso lógico controlado de acordo com as diretrizes a seguir, são sempre fornecidas em caráter individual, e em concordância com as regras estabelecidas na **Política de Segurança em Estações de Trabalho e Recursos de Computação Móvel da Omnisblue**;

VIII. Os servidores físicos da Omnisblue são atendidos por nobreaks profissionais com capacidade mínima de 4 horas;

IX. As instalações físicas da Omnisblue devem sempre estar disponibilizadas em edifícios que possuam e gerador físico de energia auxiliar;

X. O descarte de informações físicas deve ser realizado em concordância com a **Política de Descarte de Dados da Omnisblue.**

4.1.2. Controle de acesso lógico e senhas

I. Os ativos de informação devem ser acessados mediante concessão de acesso com usuário e senhas individuais e intransferíveis;

II. Toda demanda de concessão de acesso a sistemas, ativos e produtos da Omnisblue deverá ser encaminhada ao Departamento de Infraestrutura através do formulário de chamado técnico;

III. Todas as solicitações de acesso devem ser aprovadas pelo superior imediato do colaborador e pelo dono do perfil solicitado, de forma a assegurar que o acesso solicitado é o mínimo necessário para os requerimentos de negócio e funções do solicitante e que não fere os princípios de segregação de funções onde eles sejam possíveis e praticáveis;

IV. É responsabilidade do requerente, zelar pela veracidade das informações providas no formulário “SAS - Solicitação de Acesso a Sistemas”;

V. Antes de obter acesso aos sistemas de informação da Omnisblue, independente do meio de acesso (remoto ou não), os colaboradores internos, terceiros, prestadores de serviço ou parceiros comerciais necessitam assinar o “Termo de responsabilidade para uso de recurso corporativo”;

VI. Credenciais fornecidas a colaboradores internos possuirão data de expiração máxima de 180 dias, quando elas devem ser renovadas;

VII. Credenciais fornecidas a terceiros, prestadores de serviço ou parceiros comerciais, possuirão data de expiração máxima de 90 dias. Esta data poderá ser reduzida de acordo com o período de permanência do profissional na empresa ou estendida, sempre que necessário, através de solicitação formal;

VIII. Os gestores das áreas devem notificar o time de segurança da informação da empresa imediatamente sobre usuários que mudaram de área, cargo ou função ou deixaram a organização, para que as ações apropriadas sejam efetuadas;

IX. Nos casos de mudança de área, o novo gestor do colaborador deve solicitar formalmente os novos acessos requeridos pela nova função do funcionário;

X. É proibido tentar acessar recursos adicionais aos que foram atribuídos a você pelo seu superior imediato. Qualquer acesso não autorizado será considerado falta grave;

XI. Credenciais de usuários serão bloqueados após 60 dias de inatividade e removidos após 90 dias de bloqueio a menos que o usuário em questão solicite que a conta seja reativada, provando sua identidade e que o relacionamento de negócios com a empresa não mudou durante o período de inatividade;

XII. Todo usuário deve estar ciente de que suas credenciais de acesso não devem ser compartilhadas. Qualquer infração ou anormalidade no sistema será atribuída ao proprietário da credencial em uso;

XIII. É obrigatório o uso de dez (10) caracteres para a formação de uma senha de acesso;

XIV. Para os ativos internos da empresa, após cinco (5) tentativas incorretas de acesso ao sistema, a senha do usuário será bloqueada, devendo ser reativada, após trinta (30) minutos de espera;

XV. Os usuários devem verificar a notificação que é feita no início de uma sessão (quando fornecida pelo sistema em uso) referente aos dados da última utilização do sistema e notificar seu superior caso suspeite que suas credenciais tenham sido utilizadas por terceiros;

XVI. Para os ativos internos da empresa, todas as senhas possuem noventa (90) dias de validade. Após este prazo, o usuário é obrigado

a alterá-las, não sendo permitido repetir as doze (12) últimas senhas utilizadas no sistema;

XVII. Usuários nunca devem escrever ou gravar uma senha de forma desprotegia e guardá-la próxima ao dispositivo ao qual ela pertence. Senhas devem ser protegidas com o mesmo nível de proteção dado à informação que elas protegem;

XVIII. As senhas devem ser alteradas sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.

4.1.3. Criptografia de dados

I. As informações armazenadas ou transmitidas pela Omnisblue devem observar os requisitos de criptografia, dentro dos limites legais vigentes, visando maximizar o nível de confidencialidade das informações, de acordo com a classificação dos dados tratados;

II. Todas as aplicações web desenvolvidas pela Omnisblue devem ser disponibilizadas através de protocolos HTTPS;

III. Todas as aplicações web desenvolvidas pela Omnisblue devem utilizar certificados SSL assinados por autoridades certificadoras confiáveis em sistemas web, para garantir que as informações acessadas ou transmitidas não sejam interceptadas por pessoas não autorizadas;

IV. Todos os serviços de repositório de dados utilizados pela Omnisblue devem ser gerenciados por criptografia do tipo Advanced Encryption Standard de 256 bits (AES-256);

V. As estações de trabalho da Omnisblue com sistema operacional Windows (físicas ou virtuais) devem ter seus discos configurados para operarem com o BitLocker ativado;

VI. As estações de trabalho da Omnisblue com sistema operacional Linux devem ter seus discos configurados para operarem com LUKS (Linux Unified Key Setup-on-disk-format);

VII. Todas as chaves criptográficas utilizadas pela Omnisblue devem ser protegidas contra modificação e perda;

VIII. As chaves privadas e secretas devem ser protegidas contra uso ou divulgação não autorizada.

4.1.4. Mensageria eletrônica

I. A troca de mensagens eletrônicas na Omnisblue deve ocorrer de acordo com o Plano de Comunicação de cada projeto, estabelecido na etapa de planejamento dos projetos;

II. Por padrão consideramos mensagens eletrônicas válidas e oficiais as que são transmitidas através dos seguintes ativos de informação: Microsoft Teams e Microsoft Exchange;

III.Como essas ativos operam sobre a plataforma Microsoft 365, os padrões de confidencialidade associados a eles são garantidos e monitorados através do uso das ferramentas **Microsoft Defender, Microsoft Purview e DLPs (Data Loss Protection).**

4.1.5. Classificação de dados

I. Além das diretrizes definidas anteriormente, os colaboradores internos ou parceiros externos deverão ter seus acessos controlados de acordo com a classificação de dados que poderão fazer uso, garantindo requisitos de segregação de acesso e funções a depender do nível de criticidade associado às informações tratadas;

II. O acesso a esses dados deve ser realizado em concordância com a **Política de Classificação da Informação da Omnisblue**, que é associada a este guia.

4.1.6. Anonimização de dados

I. A Omnisblue poderá manter os Dados Anonimizados e versão anonimizada dos Dados Pessoais para propósitos de estatística e estudos, mesmo após solicitação de exclusão ou após o término do prazo legal de guarda;

II. Vale ressaltar que, nesse caso, quando o Dado Pessoal se torna um Dado Anonimizado, ele deixa se desse considerado um Dado Pessoal, uma vez que a privacidade do Titular de Dados está garantida, pois ele não poderá mais ser identificado por esse Dado Anonimizado.

4.1.7. Descarte de dados

I. Quando os dados e dados pessoais em tratamento pela Omnisblue não forem mais úteis e/ou a relação contratual que sustenta as atividades

de tratamento desses dados se encerrar, a Omnisblue não deve armazenar essas informações por tempo além do necessário para cumprimento de suas obrigações legais;

II. Todo o descarte de dados deve ser executado em concordância com a **Política de Descarte de Dados da Omnisblue;**

III. O reaproveitamento de discos e mídias físicas que já armazenaram informações, seja por pessoas internas ou externas à empresa, só é possível mediante procedimento de descarte e destruição das informações anteriormente presentes nesses dispositivos, garantindo que essas informações não sejam repassadas e acessadas por quem não tem permissão para vê-las. A atividade de limpeza/formatação dessas mídias deve ser realizada pelo time de Segurança da Informação da Omnisblue previamente ao reaproveitamento dos itens de configuração.

4.1.8. "Mesa limpa"

I. A Omnisblue ainda define que todos seus colaboradores e parceiros externos prestadores de serviços alocados em suas dependências realizem suas atividades de trabalho em concordância com práticas de "mesa limpa";

II. As definições e práticas a serem observadas sobre o tema estão definidas na **Política de Descarte de Dados da Omnisblue,** que está associada a este guia.

5. Medidas técnicas de integridade

5.1. Visando maximizar o nível de integridade das informações tratadas pela Omnisblue, os ativos de informação utilizados na empresa para a execução de atividades internas ou para cumprimento de obrigações contratuais com terceiros devem ser configurados atendendo aos seguintes critérios de segurança:

5.1.1. Gestão de logs

I. Os ativos de informação e as principais atividades do time de colaboradores da Omnisblue devem ser alvo de monitoria de logs de acesso e execução de rotinas;

II. Todos os ativos de informação disponibilizados na plataforma Microsoft 365 são monitorados pelo uso das ferramentas Microsoft Defender, **Microsoft Purview e DLPs (Data Loss Protection)**, garantindo a possibilidade de auditoria através da análise dos logs gerados por essas ferramentas;

III. Todos os ativos de informação disponibilizados na plataforma Oracle Cloud Infrastructure (OCI) possuem logs habilitados por padrão para fins de monitoria de infraestrutura, controle de configurações, acesso e regras de firewall;

IV. Todas as rotinas de negócio consideradas "core business" das aplicações desenvolvidas pela Omnisblue são monitoradas por aplicações de log de atividade e acesso de usuário, garantindo a possibilidade de se identificar acessos indevidos bem como históricos de execução dessas rotinas. Esses logs são persistidos na camada de Banco de Dados das respectivas aplicações;

V. Todo o acesso de configuração e deployment de aplicações desenvolvidas pela Omnisblue nos ambientes de homologação e produção são alvo de monitoria de logs;

VI. Apenas colaboradores autorizados e com acesso lógico pré-definido devem ter acesso aos logs gerenciados pela Omnisblue. O acesso a esses logs pode depender do escopo que eles estão associados.

5.1.2. Gestão de mudanças

I. Todas as mudanças realizadas em serviços e produtos tratados pela Omnisblue devem ser executadas de forma organizada, planejada e controlada;

II. Os requisitos a serem observados quanto ao controle de mudanças estão definidos na **Política de Gestão de Mudanças da Omnisblue.**

5.1.3. Gestão de horários padrão e relógios

I. Os relógios de todos os ativos de informação eletrônicos gerenciados pela Omnisblue devem ser sincronizados de acordo com o horário oficial local;

II. Essa sincronização deve ser realizada de forma automática e sua configuração está limitada aos administradores da infraestrutura da empresa.

5.1.4. Camadas de acesso a dados

I. As aplicações desenvolvidas pela Omnisblue devem seguir sempre as melhores práticas de divisão de camadas lógicas da solução, garantindo que a gravação/armazenamento dos dados gerenciados pela solução ocorra sempre a partir do tratamento prévio por camadas de negócio ou aplicação;

II. É proibido a manipulação de dados e dados pessoais diretamente nas bases de dados sem que o tratamento dessas informações passe pelas camadas de negócio ou aplicação, que devem garantir a qualidade e integridade desses dados de acordo com as regras de negócio implementadas nas aplicações.

6. Medidas técnicas de disponibilidade

6.1. Os ativos da informação gerenciados pela Omnisblue devem estar disponíveis sempre que necessário for para cumprirem seus papéis operacionais, comerciais e tecnológicos.

6.2. Visando atender aos níveis de serviço estabelecidos e acordados entre a Omnisblue e seus colaboradores e clientes, as seguintes medidas técnicas de disponibilidade são implementadas em nossos ambientes:

6.2.1. **Redundância:** Implementação de redundância nos componentes críticos dos ativos de TI em uso. Isso inclui servidores redundantes, sistemas de armazenamento em cluster e conexões de rede redundantes: Se um componente falhar, outros estarão disponíveis para assumir a carga de trabalho;

6.2.2. **Balanceamento de Carga:** Utilizamos técnicas de balanceamento de carga para distribuir a carga de trabalho entre vários servidores em regiões diferentes para computação em nuvem. Isso ajuda a evitar sobrecargas em um único servidor e mantém os serviços disponíveis, mesmo durante picos de demanda;

6.2.3. **Monitoramento de Desempenho:** Fazemos uso de ferramentas de monitoramento de desempenho que possam identificar problemas de desempenho e gargalos nos nossos ativos. Isso permite que tomemos medidas proativas para otimizar o desempenho e garantir a disponibilidade dos serviços;

6.2.4. **Planos de Continuidade de Negócios:** Fazemos uso de backups regulares dos tipos incrementais e/ou completos e realizamos testes de recuperação desses backups regularmente, em um intervalo mínimo mensal. Os arquivos de backup nunca são armazenados internamente nas dependências da Omnisblue ou nos mesmos ativos originais;

6.2.5. **Proteção contra-ataques DDoS:** Fazemos uso de medidas de proteção contra ataques de negação de serviço distribuídos (DDoS) para evitar a interrupção dos serviços. Isso envolve tanto o uso das medidas técnicas definidas no tópico a seguir como também o uso de sistemas de detecção e mitigação de DDoS, bem como serviços de mitigação baseados em nuvem.

7. Medidas técnicas de proteção contra ataques e acessos não autorizados

7.1. Toda aplicação desenvolvida pela Omnisblue para oferta ao mercado e clientes externos, e/ou os ativos de informação gerenciados e utilizados na operação da empresa devem passar por rotinas formais de teste de segurança de forma contínua;

7.2. Essas rotinas de testes e auditorias de segurança devem ser realizadas por empresa parceira externa, devidamente capacitada e com experiência comprovada no tema, e o resultado dessas rotinas de auditorias poderá endereçar mudanças arquiteturais e de infraestrutura nesses ativos de informação;

7.3. Além desses testes, a Omnisblue adota as seguintes medidas de proteção contra ataques e acessos não autorizados a seus ativos de informação:

7.3.1. **Antivírus:**

I. Estações de trabalho e servidores físicos da Omnisblue são protegidos de forma proativa pelo uso da ferramenta Trendmicro que não podem ser desabilitados por nenhum usuário.

7.3.2. **Firewall:**

I. Estações de trabalho e servidores físicos da Omnisblue são protegidos e monitorados de forma proativa pelo uso de firewall Fortigate configurados por time especializado com regras adequadas à realidade operacional da empresa e em concordância com as melhores práticas

do mercado, inclusive as estabelecidas nas normas ISO/IEC 27001 e ISO/IEC 27002;

II. Ativos da informação disponibilizados em ambiente computacional em nuvem são protegidos de forma proativa com o uso de **WAF (Web Application Firewall)** disponibilizados pela Microsoft e Oracle (respectivamente para ambientes Azure e OCI).

8. Disposições finais

8.1. Este documento deve ser conhecido por todos os colaboradores da Omnisblue e as definições aqui expostas devem ser seguidas, obrigatoriamente, sob pena de sanções internas.

8.2. As definições acima detalhadas devem ser observas em conjunto com todas as demais políticas de segurança e privacidade da informação vigentes na Omnisblue, em especial ao **Manual de Segurança da Informação da empresa**, já citado anteriormente.

8.3. O ciclo de vida deste documento está atrelado ao ciclo de vida do Manual de Segurança da Informação tal como definido no **Guia de Gerenciamento das Políticas de Segurança da Informação da Omnisblue.**

8.4. Qualquer dúvida sobre os parâmetros e definições aqui expostas deve ser dirimida com a Diretoria de Segurança e Tecnologia da Informação da empresa.

Última atualização e início de vigência desta política: 16 de junho de 2023

Versão: 1.2

omnisblue

LGPD | COMPLIANCE