# Política de Segurança da Informação em Nuvem

## Política de Segurança da Informação em Nuvem

**Tipo**: Política | PLCA-0002 | **Nº Revisão**: 7.0

**Aprovação**: CGSI | **Elaboração**: Segurança da Informação | **Classificação**: Pública

| Tipo de Controle | Propriedades de Segurança da Informação | Conceitos de Segurança Cibernética | Capacidades Organizacionais | Domínios de Segurança |
|---|---|---|---|---|
| #Preventivo | #Confidencialidade<br>#Integridade<br>#Disponibilidade | #Proteger | #Segurança_nas_relações_com_fornecedores | #Governança_e_ecossistema<br>#Proteger |

## Sumário



## 1. Objetivo

Esta política tem por objetivo estabelecer diretrizes adicionais e específicas para a solução de relacionamento com os clientes OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura que é cliente do serviço em nuvem, orientando seus colaboradores a buscar a melhoria contínua nas atividades relacionadas ao planejamento, execução, análise dos seus processos/produtos, proteção da segurança das informações geradas e o correto funcionamento do Sistema de Gestão da Segurança da Informação.

## 2. Abrangência

Este documento aplica-se as áreas:

- Segurança da Informação
- Infraestrutura Omni
- Plusoft – Cliente do Serviço em Nuvem
- E, outras soluções que estão sob à gestão da área de Infraestrutura

Orientando e fornecendo diretrizes adicionais e específicas para o ambiente de solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura que é cliente do serviço em Nuvem para o Sistema de Gestão da Segurança da Informação (SGSI).

## 3. Responsabilidades

---

# 4. Contexto da Organização

A Plusoft é uma empresa brasileira, pioneira no desenvolvimento de ferramentas multicanais para o relacionamento com clientes, oferecendo a mais completa solução Omnichannel. Com mais de 200 clientes e 70 mil usuários distribuídos entre as maiores companhias de segmentos como: varejo, saúde e indústria farmacêutica, seguros e previdência, educação, telecomunicações, serviços, alimentos e agro. Em nosso portfólio oferecemos as seguintes soluções:

- **plusoft AI**, focada em inteligência artificial a serviço do relacionamento com o cliente;
- **plusoft Social**, focada em análise, monitoramento e interação por meio de redes sociais;
- **Edusense**, plataforma virtual focada em aprendizagem social e gamificada;
- **plusoft Omni CRM**, focada na integração de todos os canais de relacionamento em uma única solução;
- **plusoft Hike,** plataforma de gerenciamento de processos focada em soluções digitais que se adaptam a modelo de negócio;
- **plusoft Trade**, focada no relacionamento e coordenação de ações com varejo;
- **plusoft Collection**, focada na orquestração digital das réguas de cobrança, aplicando modelos estatísticos e propensão pra ganho de performance operacional e financeira;
- **plusoft Geo**, plataforma especializada na expansão e logística de marcas;
- **plusoft Mkt Suite**, focada em serviços que utilizam ciência de dados com histórico de comportamentos online e offline integrado para impulsionar resultados de público e oferta.

As soluções da Plusoft garantem a seus clientes a otimização de processos nas áreas de atendimento, vendas, aprendizagem, modelagem de processos e marketing, acelerando a resolução de demandas de usuários, reduzindo custos operacionais e melhorando a percepção de consumidores com relação à marca.

Por termos acesso às informações confidenciais de clientes, fornecedores e colaboradores, há um interesse da Alta Direção em realizar a proteção dessas informações, seguindo políticas, normas e procedimentos que garantam a confidencialidade, integridade e disponibilidade delas. Desta forma, todos os controles relacionados à segurança da informação serão orquestrados por um Sistema de Gestão da Segurança da Informação que permita um processo de melhoria contínua na capacidade da organização em avaliar, detectar, mitigar os riscos e incidentes de Segurança da Informação.

---

# 5. Objetivo SI Para a Computação em Nuvem

Este documento fornece diretrizes de Segurança da Informação para a computação em nuvem onde a Plusoft Informática é cliente do Serviço em Nuvem, hospedando seus ativos da solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura, atendendo aos requisitos de um sistema de gestão de segurança da informação (SGSI).

---

# 6. Escopo

O Sistema de Gestão da Segurança da Informação engloba sistemas, conexões, integrações, processos e pessoas que interajam e possam impactar a gestão da informação processada pela Infraestrutura da solução de relacionamento com os clientes OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura, hospedada em data centers e provedores de serviços em nuvem. A solução OMNI Plusoft é a principal oferta ao mercado e a segurança em sua infraestrutura é o principal requisito solicitado pelos clientes.

---

# 7. Política de Segurança da Informação

A Política de Segurança da Informação é descrita em detalhes no documento “Política de Segurança da Informação” localizada na intranet da Plusoft. É revisada quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação, eficácia e aderência à necessidade do negócio.

---

# 8. Recursos e Organização da Segurança da Informação

O gerenciamento estruturado da Segurança da Informação endereça, monitora e controla todas as implementações relacionadas à segurança para a corporação, conforme descrito no Manual do Sistema de Gestão da Segurança da Informação, que se encontra publicada na intranet.

A Plusoft é um cliente de serviços em nuvem, celebra um contrato de prestação de serviço com um provedor de serviços em nuvem.

Como critério de seleção, o provedor de serviços em nuvem deve:

- Fornecer diversos recursos e serviços de segurança para aumentar a privacidade e controlar o acesso à rede. A segurança na nuvem é a maior prioridade.
- Ser certificado em ISO 27001, ISO 27017, ISO 27018 e PCI DSS Nível 1, contendo rigorosos controles de segurança da informação sendo avaliados por empresas de auditorias independentes.

É mandatório para Segurança da Informação definir papéis e responsabilidades para este serviço.

## 8.1. Papéis e responsabilidades

### 8.1.1. Plusoft Cliente do Serviço em Nuvem

A Plusoft assume a gestão e a responsabilidade pelo sistema operacional convidado (inclusive atualizações e patches de segurança) por outro software de aplicativo associado, bem como pela configuração do firewall do grupo de segurança fornecido pelo provedor de serviços em nuvem.

**Responsabilidade do cliente**: A responsabilidade do cliente será determinada pelos serviços da nuvem selecionados por ele. Isso determina a quantidade de operações de configuração que o cliente deverá executar como parte de suas responsabilidades de segurança.

### 8.1.2. Provedor do Serviço em Nuvem

Segurança e compatibilidade são responsabilidades compartilhadas entre o provedor de serviços em nuvem e o cliente do serviço em nuvem.

Devem ser examinados cuidadosamente e aprovados pela Segurança da Informação os serviços que foram escolhidos, pois suas respectivas responsabilidades variam de acordo com os serviços utilizados, a integração desses serviços ao seu ambiente de TI e as leis e regulamentos aplicáveis.

**Responsabilidade do provedor de serviço em nuvem**: É responsável pela proteção da infraestrutura global que subjacente à nuvem e todos os serviços oferecidos em sua nuvem. Essa infraestrutura abrange o hardware, o software, a rede e as instalações que operam os serviços.

Proteger a infraestrutura é a maior prioridade. O provedor de serviço em nuvem pode vetar a visita aos escritórios e data centers, para ter essa proteção diretamente os provedores devem disponibilizar vários relatórios de auditores independentes que verificam nossa conformidade com diversas normas e padrões de segurança em computação.

Os controles se aplicam à camada de infraestrutura e às camadas do cliente, mas em perspectivas ou contextos totalmente distintos. Em um controle compartilhado o provedor de serviços em nuvem disponibiliza os requisitos de infraestrutura e o cliente deve disponibilizar sua própria implementação de controles dentro do uso de Serviços em Nuvem. Os exemplos incluem:

- **Gerenciamento de patches:** Responsável pela aplicação de patches e pela correção de falhas na infraestrutura, mas a Plusoft é responsável pela aplicação, dos patches do seu Sistema Operacional convidado e nos seus aplicativos.
- **Gerenciamento de configuração:** Mantém a configuração dos dispositivos de infraestrutura, mas o cliente é responsável pela configuração dos seus próprios bancos de dados, aplicativos e sistemas operacionais convidados.
- **Conhecimentos e treinamento:** Treina funcionários, mas a Plusoft deve treinar seus próprios funcionários.
- **Específico do cliente (Plusoft):** controla o que é de responsabilidade exclusiva com base no aplicativo implantado nos Serviços do Provedor de Serviços em Nuvem. Os exemplos incluem: Proteção ou zona de segurança de serviços e comunicação, que pode exigir que o cliente roteie dados para ambientes de segurança específicos, ou que dívida os dados em questão entre eles.

Além de proteger essa infraestrutura global, o provedor de serviços em nuvem é responsável pela configuração de segurança dos produtos considerados serviços gerenciados que oferece.

Deve permitir a escalabilidade e a flexibilidade dos recursos baseados na nuvem com o benefício adicional de serem gerenciados e a recuperação de desastres.

No caso da maioria desses serviços gerenciados só é preciso configurar controles de acesso lógico aos recursos e proteger as credenciais de sua conta.

Como complemento aos papéis e responsabilidades entre a Plusoft, que é um cliente de serviços em nuvem e o provedor de serviços em nuvem, o provedor deve fornecer um documento onde os papéis são especificados.

| **Responsável** | **Responsabilidade** | |
|---|---|---|
| **Plusoft** | Responsável pela segurança na nuvem | Dados do Cliente |
| | | Gerenciamento da Plataforma, aplicativos, identidade e acesso |
| | | Configuração do Sistema Operacional, rede e Firewall |
| | | Dados do lado do cliente, criptografia de dados, autenticação de integridade |
| | | Proteção do tráfego de rede (criptografia / integridade / identidade) |
| **Provedor de Serviço em Nuvem** | Responsável pela segurança da nuvem | Computação, armazenamento, banco de dados, redes |
| | | Infraestrutura Global, Regiões, Zonas de Disponibilidade, Ponto de Presença |

---

# 9. Gestão da Segurança da Informação do Serviço em Nuvem

Para garantir a Segurança da Informação do Ambiente da solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura, que é um cliente do serviço em nuvem, o Comitê de Segurança da Informação existente, conforme o Manual de Gestão de Segurança da Informação adota as seguintes Normas para sustentar as diretrizes apresentadas:

- Controle de Acesso
- Gestão de Terceiros
- Gestão e Classificação da Informação

- Uso Aceitável de Ativos
- Controles Criptográficos
- Gestão de Mudanças
- Gestão de Operações
- Gestão de Atualizações e Vulnerabilidade
- Gestão de Cópias de Segurança

O sistema de Gestão da Segurança da Informação tem como referência a ISO 27001 e controles adicionais da ISO 27017.

---

## 10. Informações Armazenadas no Ambiente em Nuvem

A solução do OMNI Plusoft realiza a gestão de todos os contatos entre os nossos clientes e os seus clientes.

Estes contatos têm como principal objetivo tirar dúvidas, obter informações ou relatar problemas.

Estes contatos podem ser realizados através dos principais meios de comunicação existentes no mercado (telefone, e-mail, chat e mídias sociais).

Todas as informações armazenadas nos servidores de bancos de dados, hospedados no provedor de serviço em nuvem são confidenciais e tem acesso totalmente controlado e controles de acessos específicos, conforme as Normas Controle de Acesso e Gestão e Classificação da Informação, que estão disponíveis na Intranet da Plusoft.

---

## 11. Ativos Mantidos no Ambiente em Nuvem

Entende-se como ativo intangível todo patrimônio da Plusoft capaz de gerar receitas que não têm existência física e que sejam necessárias para o bom andamento do negócio da organização como, por exemplo, informação, marca, aplicativos, entre outros.

A proteção dos ativos intangíveis deve ser feita levando em conta os requisitos legais, as normas internas de segurança da informação e os efeitos sobre as atividades da Plusoft.

Por sermos cliente dos serviços em nuvem é essencial para a necessidade de negócios da solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura dos ativos serem mantidos no provedor de serviços em nuvem. Os ativos de informação devem observar as normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

Os ativos de informação devem ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios do PSI e das Normas de Segurança da Informação e são destinados ao uso específico, sendo vedada a utilização para fins diferentes aos interesses da organização.

As demais diretrizes sobre o uso dos ativos estão definidas na Norma de Uso Aceitável de Ativos**,** que se encontra disponível na Intranet da Plusoft.

O provedor de serviços em nuvem é apenas custodiante dos ativos de informação do OMNI Plusoft, sendo **PROIBIDO** seu acesso às informações.

Alguma situação em que o provedor de serviço em nuvem necessite acessá-la por algum motivo específico o acesso somente será permitido após alinhamento jurídico e autorização formal da Alta Direção da Plusoft.

---

## 12. Processos Executados no ambiente em Nuvem

Os processos executados no ambiente em nuvem são atividades destinadas a administração do ambiente da solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura.

Estas atividades estão definidas na Norma de Gestão de Operações**,** disponíveis na Intranet da Plusoft e os procedimentos estão disponíveis na ferramenta oficial de documentação da área de infraestrutura.

---

## 13. Usuários dos Serviços em Nuvem

O usuário é um indivíduo que utiliza ou trabalha com algum objeto ou serviço em particular. É a pessoa que utiliza um dispositivo ou computador e que realiza várias operações com diferentes propósitos.

Muitas vezes, usuário é a pessoa que tem um computador ou dispositivo eletrônico para comunicar-se com outros usuários, gerar conteúdo e documentos, utilizar softwares de diversos tipos e muitas outras ações possíveis.

No contexto em nuvem os usuários podem ser descritos de algumas formas e ter objetivos específicos, conforme descritos a seguir:

**Usuários que são administradores dos serviços em nuvem:** apenas usuários funcionários da Plusoft e membros da área de infraestrutura da solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura, devidamente identificados, tem acesso ao ambiente administrado dos serviços em nuvem, porém o acesso é restrito as informações armazenadas. O time de infraestrutura é composto apenas por administradores de rede e DBA e o seu contexto é apenas prover a gestão do ambiente computacional, hospedado no provedor de serviços em nuvem.

> **a) Provedor dos serviços em nuvem:** São responsáveis em garantir a infraestrutura do ambiente, tais como Computação, armazenamento, redes, Infraestrutura Global, Regiões, Zonas de Disponibilidade, Ponto de Presença.
>
> **b) Usuários finais:** Clientes que contratam a solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura para gerenciar suas atividades finais. Esses usuários não têm acesso administrativo ao ambiente de produção do Plusoft.

## 14. Localizações Geográficas do Provedor de Serviços em Nuvem

O provedor de serviços em nuvem deve se localizar no Brasil, a sua região (virtual) deve estar descrita em suas políticas de serviço.

Todos os data centers que oferecem os serviços em nuvem devem ter no mínimo 2 ou mais data centers distintos, que possuam redundância própria e que podem ser ativados de forma independente conforme descrito nos procedimentos de cada estratégia.

Por segurança, o provedor de serviço em nuvem, não fornece informações específicas referentes a localização dos Data centers e todo o planejamento é feito sem a necessidade de tais informações já que os serviços são ativados de forma virtual e dependem apenas de 1 conexão com a Internet.

## 15. Requisitos da Segurança da Informação do Provedor de Serviço em Nuvem

O provedor de serviços em nuvem deve ter um programa efetivo de segurança que permita que os clientes dos serviços em nuvem entendam os rígidos controles existentes para manter a segurança e a proteção dos dados na nuvem.

É necessário que o provedor de serviços em nuvem atenda os seguintes requisitos de Segurança da Informação da Plusoft, que são:

| **Requisitos de Segurança da Informação** | | **Detalhamento** |
|---|---|---|
| **Segurança física e ambiental** | Detecção e supressão de fogo | Equipamentos automáticos de detecção e supressão de fogo foram instalados para reduzir o risco. O sistema de detecção de fogo utiliza sensores de detecção de fumaça em todos os ambientes do data center, espaços de infraestrutura elétrica e mecânica, salas de resfriamento e salas de equipamento gerador. |
| | Energia | Os sistemas de energia elétrica do data center são projetados para serem totalmente redundantes e passíveis de manutenção sem impacto para as operações, 24 horas por dia e sete dias por semana.<br><br>As Unidades de Alimentação de Energia Ininterrupta (UPS) fornecem energia de apoio no caso de uma falha elétrica para cargas críticas e essenciais da empresa. |
| | Clima e temperatura | O controle climático é necessário para manter uma temperatura operacional constante para servidores e outros hardwares, o que impede o superaquecimento e reduz a possibilidade de interrupções do serviço. |
| | Gerenciamento | Monitorar os equipamentos e sistemas elétricos, mecânicos e de manutenção de funções vitais para que qualquer problema possa ser imediatamente identificado. A manutenção preventiva é executada para manter a operacionalidade contínua dos equipamentos. |
| | Descomissionamento do dispositivo de armazenamento | Quando um dispositivo de armazenamento tiver atingido o final da sua vida útil, os procedimentos do provedor de serviços em nuvem incluirão um processo de desativação, que é projetado para impedir que os dados do cliente sejam expostos a pessoas não autorizadas.<br><br>O provedor deve utilizar as técnicas detalhadas em NIST 800-88 (“Orientações para o tratamento de mídia”) como parte do processo de descomissionamento. |
| **Gerenciamento de continuidade de negócios** | Disponibilidade | Nos provedores de serviços em nuvem os seus data centers devem ser construídos em clusters em várias regiões globais. Todos os data centers estão online e a serviço dos clientes; nenhum data center está “inativo”.<br><br>Em caso de falha, processos automatizados desviam o tráfego de dados do cliente da área afetada. Os principais aplicativos são implantados em uma configuração N + 1, para que no caso de uma falha do data center, haja capacidade suficiente para permitir que o tráfego seja balanceado para os locais restantes. |
| | Resposta a incidentes | O provedor de serviços em nuvem deve ter uma equipe de gerenciamento de incidentes responsável em empregar procedimentos de diagnóstico padrão do setor para impulsionar a resolução durante eventos que afetam os negócios. Os colaboradores operacionais fornecem apoio e suporte 24h x 7 dias x 365 dias para detectar incidentes e gerenciar o impacto e a resolução. |
| | Análise Executiva de toda a empresa | O provedor de serviços em nuvem deve rever os planos de resiliência de serviços, que são também periodicamente revisados por membros da equipe de gerenciamento executivo sênior. |
| | Comunicação | O provedor de serviços em nuvem deve ter diversos métodos de comunicação interna, a fim de ajudar os funcionários a compreender suas responsabilidades e funções individuais e comunicar eventos significativos em tempo hábil. |
| **Segurança de rede** | Arquitetura de rede segura | Dispositivos de rede, como o firewall e outros dispositivos de perímetro, devem monitorar e controlar as comunicações no perímetro externo e nos principais perímetros internos da rede. Esses dispositivos de proteção de perímetro utilizam conjuntos de regras, Access Control Lists (ACLs, Listas de controle de acesso) e configurações que garantem o fluxo de informações para serviços de sistemas de informações específicos. |

| | | |
|---|---|---|
| | Pontos de acesso seguro | O provedor de serviço em nuvem deve colocar estrategicamente um número limitado de pontos de acesso na nuvem para obter um monitoramento mais amplo da comunicação e do tráfego de entrada e de saída da rede.<br><br>Esses pontos de acesso para clientes, denominados endpoints de API, permitem acesso HTTP seguro (HTTPS), permitindo-lhe estabelecer sessões seguras de comunicação com suas instâncias de computação ou armazenamento. |
| | Proteção de transmissões | O cliente de serviços em nuvem se conecta a um ponto de acesso do provedor de serviços em nuvem, esses acessos são apenas por HTTPS usando Secure Sockets Layer (SSL, Camada de conexão segura), um protocolo de criptografia destinado à proteção contra espionagem, adulteração e falsificação de mensagens. |
| | Segregação corporativa do provedor de serviços em nuvem | A rede de produção do provedor de serviços em nuvem deve ser separada da rede corporativa por meio de um complexo conjunto de dispositivos de segregação/segurança de redes.<br><br>Quando precisam ter acesso aos componentes em nuvem para sua manutenção, os desenvolvedores e administradores do provedor de serviço em nuvem que fazem parte da rede corporativa necessitam solicitá-lo explicitamente por meio do sistema de tíquetes.<br><br>Todas as solicitações são analisadas e aprovadas pelo proprietário do serviço pertinente, o cliente de serviços em nuvem. |
| | Design com tolerância a falhas | Um alto nível de disponibilidade, a infraestrutura deve ser disponibilizada em uma arquitetura de TI resiliente. O provedor de serviços em nuvem deve projetar seus sistemas para tolerar falhas do sistema ou de hardware com o mínimo de impacto para o cliente de serviços em nuvem.<br><br>Os data centers devem ser construídos em clusters em várias regiões globais. Todos os data centers estão online e a serviço dos clientes; nenhum data center está “inativo”. Em caso de falha, processos automatizados desviam o tráfego de dados do cliente da área afetada. Os principais aplicativos são implantados em uma configuração N + 1, para que no caso de uma falha do data center, haja capacidade suficiente para permitir que o tráfego seja balanceado para os locais restantes.<br><br>Deve haver flexibilidade de posicionar instâncias e armazenar dados em várias regiões geográficas e, dentro de cada região, em várias zonas de disponibilidade. Cada zona de disponibilidade é concebida como uma zona de falha independente. Isso significa que, dentro de uma região metropolitana típica, as zonas de disponibilidade são fisicamente separadas e situam-se em planícies de menor risco de inundação (a categorização das zonas de inundação varia conforme a região). Além da utilização de no-breaks discretos e geradores de backup locais, cada um deles é alimentado através de grades diferentes de utilitários independentes, o que reduz ainda mais os pontos únicos de falha.<br><br>Todas as zonas de disponibilidade são redundantemente conectadas a vários provedores de trânsito. |
| | Monitoramento e proteção da rede | O provedor de serviços em nuvem deve utilizar uma grande variedade de sistemas automatizados de monitoramento para fornecer um alto nível de disponibilidade e desempenho do serviço. |
| **Acesso à gerencia da nuvem de serviços** | Análise e auditoria de contas | As contas devem ser revistas a cada 90 dias; uma nova aprovação explícita é necessária ou o acesso ao recurso é revogado automaticamente.<br><br>O acesso também é automaticamente revogado quando o registro de um funcionário é encerrado no sistema de recursos humanos. As contas do Windows e UNIX são desabilitadas, e o sistema de gerenciamento de permissões remove o usuário de todos os sistemas.<br><br>Solicitações de alterações no acesso são capturadas no log de auditoria da ferramenta de gerenciamento de permissões. Quando ocorrem alterações na função do cargo do funcionário, a continuidade de acesso deve ser explicitamente aprovada para o recurso ou será automaticamente revogada. |
| | Política de credenciais | O provedor de serviços em nuvem, uma política de credenciais com os intervalos de expiração e as configurações necessárias. Além de complexas, as senhas devem ser alteradas a cada 90 dias. |
| | Credenciais de acesso | O provedor de serviços em nuvem deve ter diversos tipos de credenciais para autenticação no intuito de garantir que apenas os processos e usuários autorizados acessem seus recursos e sua conta.<br><br>Entre essas credenciais incluem-se senhas, chaves criptográficas, assinaturas digitais e certificados. Além disso, deve oferecer a opção de exigir multi-factor authentication (MFA, Autenticação multifator) para login em sua conta. |
| | Senhas | Uma sequência de caracteres deve ser usada para login em sua conta.<br><br>As senhas devem ter um mecanismo de senha "forte". |
| | Multi-Factor Authentication (MFA) | Código de uso único para login em sua conta no provedor de serviços em nuvem, além da senha. |

| | | |
|---|---|---|
| **Gerenciamento de alterações** | Software e Infraestrutura | O provedor de serviços em nuvem deve ter um gerenciamento de mudanças as alterações que afetam serviços de impacto para os clientes são cuidadosamente analisadas, testadas, aprovadas e claramente comunicadas.<br><br>O processo de gestão de mudanças destina-se a evitar interrupções de serviço imprevistas e manter a integridade do atendimento ao cliente.<br><br>As alterações implementadas nos ambientes de produção são:<br><br>• **Analisadas** – As análises feitas dos aspectos técnicos de uma alteração são obrigatórias.<br>• **Testadas** – Antes de aplicadas, as alterações são testadas para garantir que se comportem conforme previsto e não afetem negativamente o desempenho.<br>• **Aprovadas** – Todas as alterações devem ser autorizadas para possibilitar supervisão e compreensão apropriadas do impacto comercial. |

## 16. Gerenciamento e Monitoração dos Níveis de Serviço em Nuvem

Os provedores de Serviços em Nuvem escolhidos para hospedar os ativos da solução de relacionamento com os clientes do OMNI Plusoft ou qualquer outra solução sob à gestão da área de Infraestrutura é a AWS - Amazon e OCI – Oracle que são certificadas em ISO 27001 e seus níveis de SLA são definidos e acompanhados conforme descritos abaixo:

- O Contrato de Nível de Serviços da Amazon EC2, conforme publicado em https://aws.amazon.com/pt/ec2/sla/
- O Contrato de Nível de Serviços da Amazon S3, conforme publicado em https://aws.amazon.com/pt/s3/sla/
- O Contrato de Nível de Serviços da Oracle - OCI, conforme publicado em: Contrato de Licença e Serviços Oracle (OLSA) | Oracle Brasil, Contrato de Licença e Serviços Oracle (OLSA) V031609 | Oracle Brasil, Contrato de Licença e Serviços Oracle (OLSA) V050108 | Oracle Brasil, https://www.oracle.com/us/corporate/contracts/cloud-host-delivery-policies-br-por-3126145.pdf

## 17. Descarte dos Dados do Serviço em Nuvem

O descarte dos dados armazenados no serviço em nuvem é diferente do processo de descarte de dados realizados em ambiente físicos e exigidos na ISO 27001.

Quando a Plusoft solicita ao provedor de serviços em nuvem para realizar a exclusão/descarte dos dados armazenados, os blocos onde estão armazenados devem ser marcados como não alocados e/ou indisponíveis para uso.

O provedor de serviços em nuvem deve usar mecanismos seguros para realizar a realocação dos blocos em outro lugar. Os volumes são apresentados como dispositivos de blocos não formatados brutos, que foram limpos antes de serem disponibilizados para uso.

O provedor de serviço em nuvem determina que a mídia atingiu o fim de sua vida útil, ou identifica alguma falha de hardware, devendo seguir as técnicas detalhadas NIST SP 800 - 88 ("Diretrizes para sanitização de mídia") para destruir os dados como parte do processo de descarte do equipamento.

## 18. Avaliação de Segurança do Provedor de Serviço em Nuvem

As avaliações dos controles de segurança do provedor de serviços em nuvem são realizadas através do programa de *Compliance* que permite entender os rígidos controles existentes, mantendo a segurança e a proteção de dados na nuvem.

Conforme os sistemas forem construídos na infraestrutura da Nuvem as responsabilidades de conformidade serão compartilhadas.

O recurso de serviços tem o foco em governança e de fácil auditoria aos padrões de auditoria ou conformidade aplicáveis, os capacitadores de conformidade usufruindo dos programas tradicionais, ajudando a estabelecerem e operarem em um ambiente de controle de segurança.

O provedor de serviços em nuvem deve projetar e gerenciar suas práticas de segurança obedecendo a vários padrões de segurança do setor, entre os quais:

- SOC 1/SSAE 16/ISAE 3402 (antigo SAS70)
- SOC 2
- SOC 3
- PCI DSS, nível 1
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018

## 19. Aprovação do Documento

As aprovações desse documento são assinadas eletronicamente através do DocuSign, pelos membros do Comitê de Segurança da Informação.

## 20. Revisão e Manutenção

Este documento deverá ser revisado quando alguma mudança ocorrer na organização que mude o contexto atual.

## 20.1 Histórico de Versões

| Versão | Data | Autor | Comentários |
|---|---|---|---|
| 1.0 | 30/10/2017 | Anderson Crispim | Criação do Documento |
| 2.0 | 03/09/2018 | Anderson Crispim | Revisão do Documento |
| 3.0 | 03/09/2019 | Anderson Crispim | Revisão do Documento e alteração do item 19. APROVAÇÃO DO DOCUMENTO. |
| 3.1 | 19/02/2020 | Denise Paiva | Adequação do layout |
| 3.2 | 21/05/2020 | Patricia Albuquerque | Adequações no título e nos itens 9, 19 e 20. |
| 3.3 | 07/08/2020 | Denise Paiva | Revisão do Documento e alteração do item 19. APROVAÇÃO DO DOCUMENTO. |
| 4.0 | 03/09/2020 | Patricia Albuquerque | Revisão do Documento e alteração do item 19. APROVAÇÃO DO DOCUMENTO. |
| 4.1 | 02/06/2021 | Patricia Albuquerque | Atualização dos logos e dos aprovadores. |
| 4.2 | 17/09/2021 | Patricia Albuquerque | Adequação do layout, atualização do item 19 e revisão da cloud. |
| 4.3 | 20/09/2021 | Lucas Nogueira | Ajuste índice / sumario e revisão. |
| 5.0 | 28/09/2021 | Patricia Albuquerque | Ajuste da sigla e do item 8, referente ao Manual do Sistema de Gestão da Segurança da Informação, |
| 5.1 | 30/05/2022 | Lucas Nogueira | Remoção texto em duplicidade |
| 6.0 | 07/10/2022 | Tamara Ferreira e Patricia Albuquerque | Revisão do Documento |
| 6.1 | 07/08/2023 | Patricia Albuquerque | Adequação para ISO27001/2022 |
| 6.2 | 15/08/2023 | Alexandre Cruz e Patricia Albuquerque | Inclusão de link de SLA Oracle |
| 6.3 | 29/09/2023 | Comitê SI | Aprovação |
| 6.4 | 19/08/2024 | Lucas Nogueira | Inclusão dos demais produtos do grupo plusoft no contexto da organização. |
| 6.5 | 02/09/2024 | Alexandre Alcantara | Revisão do Documento |
| 7.0 | 06/09/2024 | Comitê de SI | Aprovação pelo Comitê de SI - 2024 |