plusoft
PEOPLE TECHNOLOGY

Segurança da Informação

Saiba como a Plusoft
protege os dados de clientes,
colaboradores e parceiros.


plusoft
PEOPLE TECHNOLOGY

índice

06
1. Plano de Continuidade de Negócio

10
3. Gestão de acessos

13
5. Como os dados ficam protegidos?

19
7. Segurança da informação (Topologia)

21
9. LGPD - Lei Geral de Proteção de Dados

09
2. Política de backup, retenção e testes

11
4. Segurança no acesso dos Produtos

16
6. Data Security

21
8. WAF (Web Application Firewall)

Na Plusoft, somos comprometidos em adotar as mais avançadas práticas de gestão da informação e controle de crises para garantir a segurança dos dados de clientes, colaboradores e parceiros que estão em nossa guarda.

Além da adoção interna de ações voltadas à segurança da informação, buscamos avaliações de órgãos externos que comprovem a excelência das nossas iniciativas. Um exemplo é a nossa certificação internacional ISO 27001:2013, concedida a organizações com elevado nível de qualidade e segurança no desenvolvimento dos seus projetos, renovada recentemente.

E quais são as ações que tomamos para resguardar as informações que estão conosco? Preparamos este ebook para apresentar como tratamos aspectos da segurança da informação, desde a política de proteção de dados a ações de proteção de senhas e medidas em caso de Disaster Recovery.

Esperamos que esse material consiga sanar suas dúvidas.

Conte conosco,

Equipe Plusoft

Certificação ISO 27001

A Plusoft é certificada ISO 27001 desde 2017 e sendo auditada anualmente desde então.

A ISO 27001 tem como objetivo a implementação de uma série de controles garantindo assim que os pilares da segurança da informação sejam estabelecidos e mantidos. Dentre as principais atividades implementadas podemos citar:

- Plano e testes de continuidade de negócio
- Teste de penetração realizado por entidade externa
- Scan de vulnerabilidade periódicos
- Plano de conscientização para colaboradores
- Gestão de parceiros e fornecedores
- Gestão de ativos e riscos
- Segurança física e lógica do ambiente
- Gestão de mudanças de todas as atividades realizadas no ambiente
- Gestão de práticas em desenvolvimento seguro
- Gestão de incidentes

Plano de Continuidade de Negócio

A Plusoft trabalha em ambientes de nuvem públicas, que contam com padrões globais e sistema autossustentado por meio de equipamentos de refrigeração e alimentação de energia redundantes, com cada equipamento possuindo um sistema de backup. Dessa forma, é possível realizar manutenções planejadas sem o desligamento do Data Center, possuindo assim Alta Disponibilidade.

Nossas aplicações são construídas de forma a garantir alta disponibilidade, utilizando múltiplas zonas de disponibilidade das clouds, respeitando as normas de Segurança e Privacidade de Dados. Apesar de todos esses cuidados, desastres podem acontecer. Por isso, a Plusoft mantém uma estratégia robusta de continuidade de negócios para os serviços e as plataformas de produção. Este plano foi desenvolvido a partir de metodologias aceitas pelo setor e engloba princípios de engenharia de alta disponibilidade.

O plano de continuidade da Plusoft contém medidas para evitar e reduzir interrupções. Ele inclui detalhes operacionais, técnicas e etapas a serem seguidas antes, durante e depois de um evento.
O plano de continuidade é constantemente revisado para atender aos rigorosos requisitos regulatórios e de governança, com testes evidenciados, ações corretivas e lições aprendidas, garantindo, assim, o aprimoramento contínuo.

Continuidade da Equipe de Operação

A nossa Equipe de Operação tem total condição de atender o cliente de forma remota, caso necessário.

Inclusive, a Plusoft já possibilita o home office com todas as garantias de segurança e as ferramentas adequadas para a realização das atividades de cada departamento.

Continuidade Técnica - Alta disponibilidade da Infraestrutura

Trabalhamos com mais de uma zona de disponibilidade para garantir que caso alguma delas sofra interrupção, automaticamente a outra passe a assumir o trabalho.

Testes desse processo são realizados e evidenciados de forma periódica para garantir que tudo está funcionando conforme o esperado.

Disaster Recovery

Disaster Recovery (DR) é o nome que se dá a um conjunto de políticas e procedimentos para permitir a recuperação ou a continuação da infraestrutura de tecnologia e sistemas vitais na sequência de um desastre natural ou provocado pelo homem. A recuperação de desastre foca na TI ou sistemas de tecnologia que suportam funções de negócio.

O plano de recuperação de desastres é composto por cenários e procedimentos, que deverão ser aplicados sempre que ocorrer uma falha devido a plano de recuperação alguma inconsistência provocada em virtude de ameaças como incêndios, inundações, vandalismo, sabotagem ou falhas de tecnologia.

Em situações de desastre em que a infraestrutura dedicada é afetada é iniciada a execução do plano de recuperação.

Tempo de Migração

Funcionamento das Aplicações plusoft Omni CRM

Recovery Time Objective (RTO)
8 horas

Recovery Point Objective (RPO)
2 horas

Durante a execução do Plano de Recuperação, é seguido um Plano de Comunicação com o objetivo de manter todas as partes envolvidas informadas sobre o andamento do processo.

Testes desse processo são realizados e evidenciados para garantir que tudo está funcionando conforme o esperado.

Alta disponibilidade: termo para nomear um sistema resistente a falhas de hardware, software e energia, cujo objetivo é manter os serviços disponibilizados o máximo de tempo possível.

Zonas de disponibilidades das clouds: podem ser descritas como "ilhas" dentro de uma plataforma de computação em nuvem, que permitem aos usuários alocar sua base de dados em um data center mais próximo, obtendo vantagens como otimização de tempo para execução de tarefas.

Recovery Time Objective (RTO): indicador criado para medir o limite de tempo que um sistema ou uma informação pode ficar indisponível após uma falha.

Recovery Point Objective (RPO): indicador que aponta a quantidade (ou tempo) de informações que podem ser perdidas caso uma falha grave ocorra dentro do sistema.

Política de backup, retenção e testes

As cópias de segurança têm o objetivo de garantir a recuperação de dados essenciais à infraestrutura de produção quando esses, por qualquer motivo, não possam ser obtidos das bases em que originalmente foram armazenados.

O gerenciamento das cópias de segurança é realizado em uma plataforma de armazenamento de objetos, que é gerenciada pelo provedor de serviços em nuvem. Essa plataforma oferece altíssima escalabilidade, confiabilidade, velocidade e grande resiliência, sendo distribuída automaticamente em mais de uma instalação física separada geograficamente dentro de uma mesma região.

Todos os dados armazenados da cópia de segurança são criptografados, aumentando a segurança das informações coletadas. Testes desse processo de backup são realizados e evidenciados para garantir que a integridade dos backups.

Peridiocidade	Tipo	Retenção	Periodicidade Teste Recuperação
Diária	Completo	14 dias	Mensal (Aleatória)
Mensal	Completo	13 meses (último dia de cada mês)	Mensal (Aleatória)
Semanal	Completo	4 semanas (a cada Domingo)	Mensal (Aleatória)

Gestão de acessos

A Plusoft segue um processo de segmentação de responsabilidades e acessos na Gestão da Infraestrutura, com objetivo de atribuir permissão de acessos compatível com a função e a necessidade das áreas. Dentro desta política, cada colaborador poderá visualizar e/ou alterar apenas as configurações de sua incumbência.

O acesso ao nosso parque tecnológico é feito por meio de autenticação centralizada (SSO), garantindo assim um ponto único de controle.

A Plusoft implementa uma política de senha complexa, seguindo as boas práticas de mercado, incluindo alterações regulares e não possibilidade de reutilização.

Segurança no acesso dos Produtos

Política de senha

Por que senhas importam tanto?
O acesso não autorizado a um dispositivo (como computador, celular, tablet etc) ou a uma conta é um problema potencialmente grave para qualquer um. Dependendo do que for acessado, é possível conseguir informações confidenciais e realizar ações no nome da outra pessoa.

A senha é a primeira frente de defesa contra uma tentativa de invasão. Ela é uma das formas de validar que um cliente ou usuário é ele mesmo.

Pensando nisso, a Plusoft conta com uma política de senha em seus produtos, permitindo que o cliente configure a sua política de senha forte para o acesso dos seus usuários.

Restrição de IP

Complementando a política de senha forte, nossos produtos contam também com uma segurança adicional aos acessos, que é a Restrição por IP. Nessa funcionalidade, o cliente pode montar uma lista com os IPS que têm permissão de acesso. Assim, qualquer outra solicitação vinda de um IP diferente aos que foram cadastrados é negada.

Autenticação por meio do SSO

O SSO (Single sign-on) é uma solução tecnológica que permite que esses aplicativos usem a mesma senha para todos os acessos de forma segura e transparente. Ou seja, com o SSO, o usuário digita apenas uma senha quando faz o primeiro acesso e depois vai abrindo os demais aplicativos sem necessidade de digitar novamente a senha.

Pensando nisso, nossos produtos estão prontos para usar essa tecnologia, tornando o acesso mais seguro e facilitando o controle das senhas, onde o controle de acesso não será mais realizado dentro do nosso produto, e, sim, pelo processo interno do cliente usando já suas políticas seguras para senhas.

Como os dados ficam protegidos dentro da infraestrutura SaaS?

Há duas arquiteturas muito conhecidas e utilizadas pelas empresas, a multi-tenant e a multi-instance. A primeira é reconhecida por ter apenas uma aplicação e uma base dados para todos os clientes, o que os separa é uma chave estrangeira e os relacionamentos no banco de dados.

Já a arquitetura multi-instance aloca instâncias de servidores e banco de dados por cliente. Com esta arquitetura é possível ter um isolamento completo dos dados e a possibilidade de ter configurações e otimizações de forma individual. Esta é a forma que a Plusoft trabalha.

Entenda melhor os benefícios e porque optamos por ela:

Data Isolation

Cada companhia ou time designado possui seu próprio banco de dados e infraestrutura, resultando em um isolamento total dos dados e fornecendo garantia de confidencialidade para os clientes.

Escalabilidade simplificada

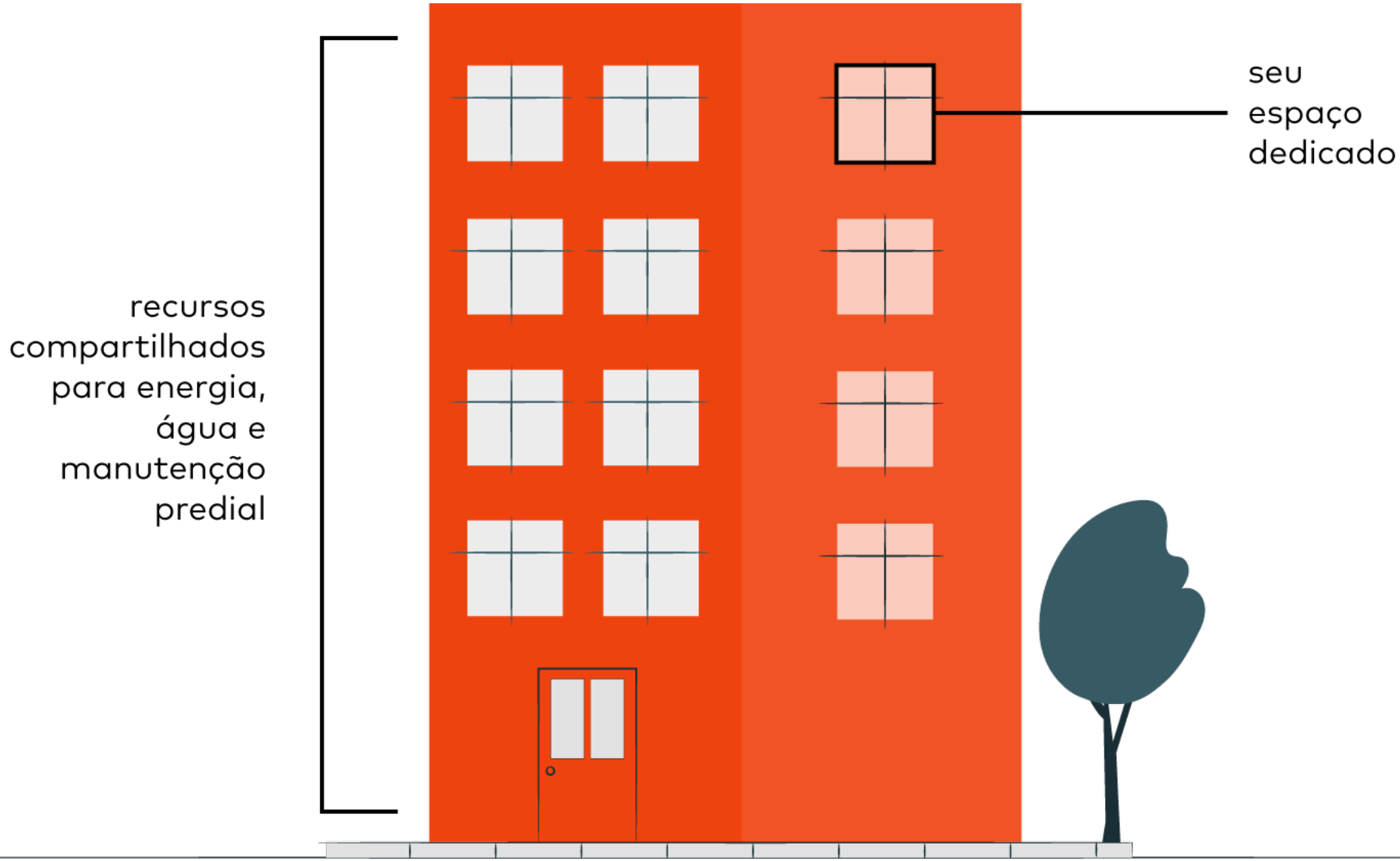
Para aumentar os recursos, o processo se torna mais simples, já que apenas a sua infraestrutura passará por modificações, podendo alocar mais CPU, RAM ou armazenamento de acordo com suas necessidades e interesses.

Aumento na disponibilidade geral

Se uma das instâncias dos clientes falhar, não há motivos para se preocupar com toda a sua base, já que esse problema não afetará todos os outros clientes. Tornando-se assim, mais fácil de ser resolvida e reestabelecida.

Alta personalização

Cada um dos clientes que possuem instâncias pode receber uma personalização de seu SaaS, que podem ser facilmente transformadas em argumentos de negócios. Funcionalidades dedicadas, atualizações programadas e outras personalizações podem ser incluídas.


seu
espaço
dedicado
recursos
compartilhados
para energia,
água e
manutenção
predial

Data Security

O que é a Segurança de Dados (Data Security)?

A segurança dos dados é um conjunto de processos e tecnologias que protegem os dados contra acessos indevidos, bem como a modificação ou divulgação de informações confidenciais.

A segurança dos dados pode ser aplicada usando uma série de técnicas e tecnologias, incluindo controles administrativos, segurança física, controles lógicos, processos organizacionais e outras técnicas de salvaguarda, que limitam o acesso a usuários ou processos não autorizados ou maliciosos.

O objetivo principal da segurança de dados é proteger os dados que uma organização coleta, armazena, cria, recebe ou transmite. Seguindo esse princípio, a Plusoft trabalha de forma segura em seu parque tecnológico e seus produtos, com implementação de vários processos de Segurança:

Database Encryption

Implementação de uma criptografia transparente nos bancos de dados (TDE) nos arquivos de dados com objetivo de proteger os dados em repouso.

Database Audit

Criação de controles sobre os acessos e comandos executados nos bancos de dados, visando posterior auditoria das ações executadas.

Data Sanitization

Execução de um embaralhamento de dados, com o objetivo de mascarar a informação sensível do cliente, caso seja necessária uma movimentação de ambiente de produção para ambiente de homologação.

Enterprise key management

Desenvolvimento de um local seguro e com acesso restrito, para armazenamento das chaves administrativas de acesso aos bancos de dados.

Monitoramento 24x7

A Plusoft tem implementado em sua estrutura monitoramento 24x7. Este processo de monitoração visa garantir a disponibilidade e a rápida estabilização do ambiente em caso de eventual problema. Esta monitoração está focado em monitoração de infraestrutura(técnica) e negócio(aplicação).

NOC (Network operation center)
O NOC tem como responsabilidade a monitoração dos ambientes de infraestrutura garantindo que os equipamento e serviços estejam em execução de acordo com o estabelecido, gerando alertas para a equipe de monitoração e garantindo a rápida estabilização e resolução.

BOC (Business operation center)
O BOC tem como responsabilidade a monitoração de negócio da aplicação garantindo que a aplicação esteja executado e respondendo conforme esperado e garantindo que divergências de comportamento sejam alertadas para a equipe de monitoração.

Topologia

- As requisições chegam na cloud através da resolução de DNS;
- Todas as requisições são direcionadas ao WAF, que realizará toda a análise do tráfego e recusará o que for indevido ou direcionará para o loadbalancer as requisições válidas;
- O loadbalancer, por sua vez, através do healcheck enviará as requisições para os servidores de aplicação disponíveis na sua zona de disponibilidade específica;
- Cada região possui uma estrutura replicada, tornando assim, o ambiente altamente redundante;
- Os bancos de dados independente da região depositam os backups e arquives no storage para futura utilização caso necessário.


plusoft
OMNI CRM
WAF
Load
Balancer
Região 1
Server
App.
Server
App.
Banco
de dados
Região 2
Server
App.
Server
App.
Banco
de dados
Storage

WAF

(Web Application Firewall)

O Firewall de aplicativo da web (Web Application Firewall - WAF) é um firewall que monitora, filtra e bloqueia pacotes de dados durante o tráfego das requisições. Esta ferramenta visa proteger a aplicação contra eventual tentativa em explorar vulnerabilidade da aplicação.

LGPD

Lei de Proteção de Dados

LGPD é a sigla de Lei Geral de Proteção de Dados (Lei 13.709) sancionada em 14de agosto de 2018 e que entrou em vigor em agosto de 2020. Seu principal objetivo é garantir transparência e os devidos controles no uso dos dados das pessoas físicas.

A Plusoft atuou fortemente no processo de adequação dos processos internos e em seus produtos para garantir a conformidade a conformidade da lei.

Desta forma os nossos clientes possuem a possibilidade de:

Determinar a base legal, finalidade e vigência dos dados

Anonimização/ bloqueio temporário dos dados de acordo com a solicitação do titular

Consulta dos dados dos titulares

Definição de base legal para campanha para realizar opt-in e opt-out

A Plusoft é uma das maiores empresas de Human Experience (HX). A companhia trabalha diariamente para ajudar a satisfazer o que mais importa na cadeia de valor das empresas: as pessoas.

A Plusoft domina as melhores tecnologias para munir as empresas com a principal ferramenta para obter performance nesse mundo cada vez mais impessoal: os relacionamentos de valor. A Plusoft é People Technology.

A empresa é especialista em soluções Omnichannel de Customer Relationship Management (CRM) para todos os mercados (seguros, alimentação, telecomunicações, financeiro, entre outros).

Com mais 30 anos de atuação no mercado, a Plusoft é a primeira companhia nacional do segmento a conquistar a certificação internacional ISO 27001:2013, concedido a organizações com elevado nível de qualidade e segurança no desenvolvimento de seus projetos.

A Plusoft possui uma plataforma com diversas soluções, entre elas a **plusoft Omni CRM**, um dos mais completos softwares de relacionamento com o cliente, a **plusoft Social**, serviço de gerenciamento de relacionamento com os clientes de redes sociais, a **plusoft AI**, solução de chabots com inteligência artificial, contando inclusive com um Natural Language Processing (NLP) próprio, a **plusoft inPaaS**, conjunto de soluções digitais customizáveis em low-code; **plusoft Ed Tech**, responsável por uma plataforma de educação digital; e a **plusoft DTM**, que utiliza ciência de dados para impulsionar campanhas de marketing.

plusoft

PEOPLE TECHNOLOGY


plusoft
PEOPLE TECHNOLOGY