

# RELATÓRIO DE ANÁLISE DE CONFIABILIDADE DE ATIVOS DE INFORMAÇÃO – VISÃO EXECUTIVA

## Caixa Vida Previdência (CVP) | Omnisblue

### Apresentação do projeto

O projeto associado a este documento trata da realização de *atividades de consultoria especializada em diversas disciplinas técnicas visando apoiar a CVP a maximizar os resultados de seu programa de adequação a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018).*

### Objetivos do documento

- Documentar o resultado obtido após análise inicial do nível de CONFIABILIDADE dos ativos de informação eletrônicos previamente mapeados pela **CVP**.
- Apresentar uma visão executiva centralizada sobre os aspectos de CONFIDENCIALIDADE, INTEGRIDADE e DISPONIBILIDADE da informação desses ativos a partir da análise técnica e funcional das informações fornecidas pela **CVP**.

### Fundamentos legais e padrões técnicos

As análises e definições presentes neste documento estão fundamentadas na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18), nos parâmetros definidos pela norma ISO/IEC 27.001, nas práticas previstas no NIST CyberSecurity Framework (CSF) 2.0 e pelas estratégias definidas no framework de adequação à LGPD de propriedade da Omnisblue, apresentado para o time da CVP ainda nas tratativas comerciais pré-projeto e, posteriormente, em maiores detalhes durante reuniões de alinhamento entre as partes.

### Resumo das atividades e métrica utilizada

A Omnisblue recebeu, em 24/05/24, o arquivo Mapeamento.zip contendo uma série de planilhas que elencam uma análise prévia sobre aspectos de segurança da informação realizada pelo time da CVP. A partir de um alinhamento prévio entre as partes, a Omnisblue apontou, dessa série de planilhas, um total de 29 ativos de informação reconhecidos e, desses, a CVP elencou um subtotal de 14 ativos a serem analisados.

A partir dessa lista reduzida de ativos prioritários (14 ativos), a CVP forneceu, a pedido da Omnisblue, dados adicionais sobre esses ativos, como descrição e informações sobre a estratégia de gestão deles atualmente em vigor na empresa, e o time técnico da Omnisblue passou então a analisar essa lista, cruzando informações já produzidas pela CVP com padrões e referências utilizadas pela Omnisblue visando analisar o nível de confiabilidade desses ativos de informação.

Tal como combinado entre as partes, essa análise, aqui documentada, traz uma visão executiva sobre os aspectos de CONFIDENCIALIDADE, INTEGRIDADE e DISPONIBILIDADE da informação desses ativos de informação priorizados pelo time da CVP.

Para maior entendimento dos resultados, é imperativo entendermos que consideramos, aqui, o nível de CONFIABILIDADE da informação de um determinado ativo como a soma do nível de CONFIDENCIALIDADE, INTEGRIDADE e DISPONIBILIDADE da informação desse ativo, tal como ilustrado a seguir:

$$Ncb = Ncf + Nint + Ndisp$$

Onde:

- a) **Ncb** é o nível de CONFIABILIDADE do ativo, medida que indica o quanto confiável a informação contida nesse ativo é;
- b) **Ncf** é o nível de CONFIDENCIALIDADE, onde entendemos os aspectos do ativo que tratam da propriedade em que a informação ali tratada não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados;
- c) **Nint** é o nível de INTEGRIDADE, onde entendemos os aspectos do ativo que garantem que ele está correto e consistente com o estado ou a informação pretendida, e busca assegurar que sejam prevenidas modificações não autorizadas em dados ali tratados;
- d) **Ndisp** é o nível de DISPONIBILIDADE, onde entendemos os aspectos do ativo que tratam da propriedade em que a informação ali tratada é acessível e utilizável sob demanda por uma entidade, e garante que o ativo (e seus dados) está funcionando (disponível) quando necessário.

A análise da Omnisblue foi focada nos parâmetros **Ncf**, **Nint** e **Ndisp**, classificando-os em ALTO, MÉDIO e BAIXO.

A partir dessas classificações, obtém-se o **Ncb**, também classificado em ALTO, MÉDIO e BAIXO, mas de forma automática, considerando que o **Ncb** é igual ao MENOR parâmetro obtido nos índices **Ncf**, **Nint** e **Ndisp** do ativo. Isso significa que, por exemplo, para um determinado ativo com **Ncf** e **Nint** = ALTO, mas com **Ndisp** = MÉDIO, o **Ncb** desse ativo será MÉDIO (o menor índice obtido).

Para se obter os valores **Ncf**, **Nint** e **Ndisp**, a equipe da Omnisblue utilizou um checklist de melhores práticas de segurança da informação associadas a cada um desses parâmetros e classificadas entre OBRIGATÓRIAS e DESEJÁVEIS, de acordo com o que está demonstrado em cada planilha de análise anexa.

Essas práticas foram confrontadas com o estado atual da prática delas em cada um dos ativos analisados, utilizando como fonte de informação as planilhas fornecidas pela CVP. A regra utilizada para a classificação de cada parâmetro foi a seguinte:

- a) Um determinado **Ncf**, **Nint** ou **Ndisp** foi considerado ALTO sempre que TODAS AS PRÁTICAS OBRIGATÓRIAS forem encontradas em uso para um determinado ativo;
- b) Um determinado **Ncf**, **Nint** ou **Ndisp** foi considerado MÉDIO sempre que ao menos 50% de TODAS AS PRÁTICAS OBRIGATÓRIAS forem encontradas em uso para um determinado ativo;
- c) Um determinado **Ncf**, **Nint** ou **Ndisp** foi considerado BAIXO sempre que verificado um uso abaixo de 50% das PRÁTICAS OBRIGATÓRIAS para um determinado ativo.

## Lista de ativos de informação analisados

Os seguintes ativos foram objeto da análise aqui detalhada:

Ativos de informação eletrônicos priorizados									
Título	Subtipo	Descrição	Responsável atual	E-mail do responsável atual	Áreas mantenedoras	Áreas usuárias	Mantido por time interno?	Hospedado em ambiente próprio?	
AIC	SISTEMA VENDA PRODUTOS CAIXA SEGUROS	Venda no balcão das agências do Banco CEF	Andrea Costa	<a href="mailto:andre.costa@caixavidaeprevencia.com.br">andre.costa@caixavidaeprevencia.com.br</a>	GEFEN	GEPOF	Sim	Não - ambiente gerenciado pela CNP Seguros	
KIPREV	SISTEMA PROCESSAMENTO PREVIDÊNCIA	Sistema de processamento de previdência privada	Janaina Rabelo	<a href="mailto:janaina.rabelo@caixavidaeprevencia.com.br">janaina.rabelo@caixavidaeprevencia.com.br</a>	GETIP	Não identificado	Sim	Não - ambiente gerenciado pela CNP Seguros	
SALESCFORCE	SISTEMA DE ATENDIMENTO DOS CLIENTES	CRM	Flavio Goulart	<a href="mailto:flavio.goulart@caixavidaeprevencia.com.br">flavio.goulart@caixavidaeprevencia.com.br</a>	GEFEN	Não identificado	Sim	Não - ambiente gerenciado pela CNP Seguros	
SAP	SISTEMA FINANCEIRO DA COMPANHIA	Sistema Financeiro	Maximiliano Netto	<a href="mailto:maximiniano.netto@caixavidaeprevencia.com.br">maximiniano.netto@caixavidaeprevencia.com.br</a>	GEPES, GEGOP	Não identificado	Sim	Não - ambiente gerenciado pela CNP Seguros	
SMART	SISTEMA DE PRESTAMISTA	Processamento das vendas de Prestamista	Hebert Cruz	<a href="mailto:hebert.cruz@caixavidaeprevencia.com.br">hebert.cruz@caixavidaeprevencia.com.br</a>	GETIC	Não identificado	Sim	Não - ambiente gerenciado pela CNP Seguros	
SIAS	SISTEMA DE VIDA	Seguro de Vida	Lelys Junior	<a href="mailto:lelys.junior@caixavidaeprevencia.com.br">lelys.junior@caixavidaeprevencia.com.br</a>	GETIV	Não identificado	Sim	Não - ambiente gerenciado pela CNP Seguros	
Portal Vendas	SISTEMA VENDA PRODUTOS CAIXA SEGUROS	Vendas Online	Andrea Costa	<a href="mailto:andre.costa@caixavidaeprevencia.com.br">andre.costa@caixavidaeprevencia.com.br</a>	GEFEN	GEPOF	Sim	Não - ambiente gerenciado pela CNP Seguros	
Área Logada	SISTEMA PARA CONSULTA DOS CLIENTES DOS PRODUTOS ADQUIRIDOS	Sistema de Consulta dos clientes	Andrea Costa	<a href="mailto:andre.costa@caixavidaeprevencia.com.br">andre.costa@caixavidaeprevencia.com.br</a>	GEFEN	GEPOF	Sim	Não - ambiente gerenciado pela CNP Seguros	
Autocompras	SISTEMA DE VENDA ONLINE PRODUTOS CAIXA SEGURO	Venda Online	Andrea Costa	<a href="mailto:andre.costa@caixavidaeprevencia.com.br">andre.costa@caixavidaeprevencia.com.br</a>	GEFEN	GEPOF	Sim	Não - ambiente gerenciado pela CNP Seguros	

#### Ativos de informação eletrônicos priorizados

Título	Subtipo	Descrição	Responsável atual	E-mail do responsável atual	Áreas mantenedoras	Áreas usuárias	Mantido por time interno?	Hospedado em ambiente próprio?
<b>Portal Economiário</b>	PORTAL POS VENDA DO ECONOMIARIO	Venda Online	Andrea Costa	<a href="mailto:andre.costa@caixavidaeaprevidencia.com.br">andre.costa@caixavidaeaprevidencia.com.br</a>	GEFEN	GEPOF	Sim	Não - ambiente gerenciado pela CNP Seguros
<b>Portal PJ</b>	PORTAL DE ADM DO CLIENTES B2B	Vendas Online B2B	Andrea Costa	<a href="mailto:andre.costa@caixavidaeaprevidencia.com.br">andre.costa@caixavidaeaprevidencia.com.br</a>	GEFEN	GEPOF	Sim	Não - ambiente gerenciado pela CNP Seguros
<b>PowerBI</b>	INFORMAÇÕES GERENCIAIS	Relatórios Online	Leandro Branquinho	<a href="mailto:leandro.branquinho@caixavidaeaprevidencia.com.br">leandro.branquinho@caixavidaeaprevidencia.com.br</a>	GERESD	TODA COMPANHIA	Sim	Não - ambiente gerenciado pela CNP Seguros
<b>DataStage</b>	TRANSFORMAÇÃO DA INFORMAÇÃO	Formatação das informações da companhia	Leandro Branquinho	<a href="mailto:leandro.branquinho@caixavidaeaprevidencia.com.br">leandro.branquinho@caixavidaeaprevidencia.com.br</a>	GERESD	GERESD	Sim	Não - ambiente gerenciado pela CNP Seguros
<b>FPW</b>	SISTEMA RH, FOLHA DE PAGAMENTO ENTRE OUTROS	Recursos Humanos	Camila Ramos	<a href="mailto:camila.ramos@caixavidaeaprevidencia.com.br">camila.ramos@caixavidaeaprevidencia.com.br</a>	GEPES	GEPES	Sim	Não - ambiente gerenciado pela CNP Seguros

## Análise de confiabilidade dos ativos

**Observação:** os detalhes dos parâmetros analisados para cada ativo podem ser encontrados na planilha anexa a este relatório.

### ATIVO: AIC

Título do ativo	AIC
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	SISTEMA VENDA PRODUTOS CAIXA SEGUROS - Venda no balcão das agências do Banco CEF

Responsável interno do ativo	Andrea Costa
------------------------------	--------------

Nível de confiabilidade do ativo	Médio
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, monitoramento de acessos realizados na aplicação, acesso a aplicação usando MFA/Recaptcha e uma solução de prevenção contra perda de dados (DLP) implementada.
Nível de INTEGRIDADE	Médio
Análise do nível de INTEGRIDADE da informação do ativo	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, controle de versões e auditorias das alterações nos dados da aplicação, além da implementação de redundâncias e testes de consistência nos dados e nos backups.
Nível de DISPONIBILIDADE	Médio
Análise do nível de DISPONIBILIDADE da informação do ativo	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, lista de controle de acesso (ACLs), testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.

**ATIVO: KIPREV**

<b>Título do ativo</b>	<b>KIPREV</b>
<b>Tipo do ativo</b>	Eletrônico
<b>Subtipo do ativo</b>	Sistema de gestão
<b>Descrição do ativo</b>	SISTEMA PROCESSAMENTO PREVIDENCIA - Sistema de processamento de previdência privada

<b>Responsável interno do ativo</b>	Janaina Rabelo
-------------------------------------	----------------

<b>Nível de confiabilidade do ativo</b>	<b>Médio</b>
<b>Nível de CONFIDENCIALIDADE</b>	<i>Médio</i>
<b>Análise do nível de CONFIDENCIALIDADE da informação do ativo</b>	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, acesso a aplicação usando MFA/Recaptcha, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.
<b>Nível de INTEGRIDADE</b>	<i>Médio</i>
<b>Análise do nível de INTEGRIDADE da informação do ativo</b>	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, lista de controle de acesso (ACLs), testes frequentes de restauração, controle de versões e auditorias das alterações nos dados da aplicação, além da implementação de redundâncias e testes de consistência nos dados e nos backups.
<b>Nível de DISPONIBILIDADE</b>	<i>Médio</i>
<b>Análise do nível de DISPONIBILIDADE da informação do ativo</b>	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.

**ATIVO: SAP**

<b>Título do ativo</b>	SAP
<b>Tipo do ativo</b>	Eletrônico
<b>Subtipo do ativo</b>	ERP
<b>Descrição do ativo</b>	SISTEMA FINANCEIRO DA COMPANHIA

<b>Responsável interno do ativo</b>	Maximiliano Netto
-------------------------------------	-------------------

<b>Nível de confiabilidade do ativo</b>	<b>Médio</b>
<b>Nível de CONFIDENCIALIDADE</b>	<i>Médio</i>
<b>Análise do nível de CONFIDENCIALIDADE da informação do ativo</b>	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, acesso a aplicação usando MFA/Recaptcha, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.
<b>Nível de INTEGRIDADE</b>	<i>Médio</i>
<b>Análise do nível de INTEGRIDADE da informação do ativo</b>	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, controle de versões e auditorias das alterações nos dados da aplicação, além da implementação de redundâncias e testes de consistência nos dados e nos backups.
<b>Nível de DISPONIBILIDADE</b>	<i>Médio</i>
<b>Análise do nível de DISPONIBILIDADE da informação do ativo</b>	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.

## ATIVO: SMART

Título do ativo	SMART
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	SISTEMA DE PRESTAMISTA - Processamento das vendas de Prestamista

Responsável interno do ativo	Hebert Cruz
------------------------------	-------------

Nível de confiabilidade do ativo	Baixo
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	<p>Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, acesso a aplicação usando MFA/Recaptcha, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.</p>
Nível de INTEGRIDADE	Baixo
Análise do nível de INTEGRIDADE da informação do ativo	<p>Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, controle de versões e auditorias das alterações nos dados da aplicação, além da implementação de redundâncias e testes de consistência nos dados e nos backups.</p>
Nível de DISPONIBILIDADE	Médio
Análise do nível de DISPONIBILIDADE da informação do ativo	<p>Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.</p>

## ATIVO: SIAS

Título do ativo	SIAS
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	SISTEMA DE VIDA - Seguro de Vida

Responsável interno do ativo	Lelys Junior
------------------------------	--------------

Nível de confiabilidade do ativo	Baixo
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	<p>Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, acesso a aplicação usando MFA/Recaptcha, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.</p>
Nível de INTEGRIDADE	Baixo
Análise do nível de INTEGRIDADE da informação do ativo	<p>Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, controle de versões e auditorias das alterações nos dados da aplicação, além da implementação de redundâncias e testes de consistência nos dados e nos backups.</p>
Nível de DISPONIBILIDADE	Médio
Análise do nível de DISPONIBILIDADE da informação do ativo	<p>Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.</p>

## ATIVO: Portal de Vendas

<b>Título do ativo</b>	<b>Portal de Vendas</b>
<b>Tipo do ativo</b>	Eletrônico
<b>Subtipo do ativo</b>	Sistema de gestão
<b>Descrição do ativo</b>	SISTEMA VENDA PRODUTOS CAIXA SEGUROS - Vendas Online

<b>Responsável interno do ativo</b>	Andrea Costa
-------------------------------------	--------------

<b>Nível de confiabilidade do ativo</b>	<b>Médio</b>
<b>Nível de CONFIDENCIALIDADE</b>	<b>Médio</b>
<b>Análise do nível de CONFIDENCIALIDADE da informação do ativo</b>	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, acesso a aplicação usando MFA/Recaptcha, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.
<b>Nível de INTEGRIDADE</b>	<b>Médio</b>
<b>Análise do nível de INTEGRIDADE da informação do ativo</b>	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, auditorias das alterações nos dados da aplicação, logs de acesso a aplicação, controle de acesso baseado em funções (RBAC), além da implementação de redundâncias e testes de consistência nos dados e nos backups.
<b>Nível de DISPONIBILIDADE</b>	<b>Médio</b>
<b>Análise do nível de DISPONIBILIDADE da informação do ativo</b>	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.

## ATIVO: Área Logada

Título do ativo	Área Logada
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	SISTEMA PARA CONSULTA DOS CLIENTES DOS PRODUTOS ADQUIRIDOS

Responsável interno do ativo	Andrea Costa
------------------------------	--------------

Nível de confiabilidade do ativo	Alto
Nível de CONFIDENCIALIDADE	Alto
Análise do nível de CONFIDENCIALIDADE da informação do ativo	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada alta, pois grande parte das medidas técnicas obrigatórias para este ativo foram atendidas.
Nível de INTEGRIDADE	Alto
Análise do nível de INTEGRIDADE da informação do ativo	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi alta, pois grande parte das medidas técnicas obrigatórias para este ativo foram atendidas.
Nível de DISPONIBILIDADE	Alto
Análise do nível de DISPONIBILIDADE da informação do ativo	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi alta, pois grande parte das medidas técnicas obrigatórias para este ativo foram atendidas.

## ATIVO: Auto Compras

Título do ativo	AutoCompras
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	SISTEMA DE VENDA ONLINE PRODUTOS CAIXA SEGURO - Venda Online

Responsável interno do ativo	Andrea Costa
------------------------------	--------------

Nível de confiabilidade do ativo	Médio
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	<p>Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.</p>
Nível de INTEGRIDADE	Médio
Análise do nível de INTEGRIDADE da informação do ativo	<p>Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, auditorias das alterações nos dados da aplicação, controle de acesso baseado em funções (RBAC), além da implementação de redundâncias e testes de consistência nos dados e nos backups.</p>
Nível de DISPONIBILIDADE	Médio
Análise do nível de DISPONIBILIDADE da informação do ativo	<p>Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.</p>

## ATIVO: Data Stage

<b>Título do ativo</b>	<b>Data Stage</b>
<b>Tipo do ativo</b>	Eletrônico
<b>Subtipo do ativo</b>	Sistema de gestão
<b>Descrição do ativo</b>	TRANSFORMAÇÃO DA INFORMAÇÃO - Formatação das informações da companhia

<b>Responsável interno do ativo</b>	Leandro Doutor Branquinho
-------------------------------------	---------------------------

<b>Nível de confiabilidade do ativo</b>	<b>Médio</b>
<b>Nível de CONFIDENCIALIDADE</b>	<b>Médio</b>
<b>Análise do nível de CONFIDENCIALIDADE da informação do ativo</b>	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: logs de acesso, criptografia de dados em repouso e trânsito para esse ativo, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.
<b>Nível de INTEGRIDADE</b>	<b>Médio</b>
<b>Análise do nível de INTEGRIDADE da informação do ativo</b>	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, logs de acesso e auditorias das alterações nos dados da aplicação, RECAPTCHA para mitigar riscos de ataques DDOS, além da implementação de redundâncias e testes de consistência nos dados e nos backups.
<b>Nível de DISPONIBILIDADE</b>	<b>Médio</b>
<b>Análise do nível de DISPONIBILIDADE da informação do ativo</b>	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.

## ATIVO: FPW

Título do ativo	FPW
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	SISTEMA RH, FOLHA DE PAGAMENTO ENTRE OUTROS

Responsável interno do ativo	Camila Ramos
------------------------------	--------------

Nível de confiabilidade do ativo	Médio
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: logs de acesso, criptografia de dados em repouso e trânsito para esse ativo, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.
Nível de INTEGRIDADE	Médio
Análise do nível de INTEGRIDADE da informação do ativo	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, logs de acesso e auditorias das alterações nos dados da aplicação, RECAPTCHA para mitigar riscos de ataques DDOS, controle de acesso baseado em funções (RBAC), além da implementação de redundâncias e testes de consistência nos dados e nos backups.
Nível de DISPONIBILIDADE	Médio
Análise do nível de DISPONIBILIDADE da informação do ativo	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.

## ATIVO: Portal Economiario

Título do ativo	Portal Economiario
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	PORTAL POS VENDA DO ECONOMIARIO - Vendas Online

Responsável interno do ativo	Andrea Costa
------------------------------	--------------

Nível de confiabilidade do ativo	Médio
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	<p>Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: logs de acesso, criptografia de dados em repouso para esse ativo e uma solução de prevenção contra perda de dados (DLP) implementada.</p>
Nível de INTEGRIDADE	Médio
Análise do nível de INTEGRIDADE da informação do ativo	<p>Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, auditorias das alterações nos dados da aplicação, controle de acesso baseado em funções (RBAC), além da implementação de redundâncias e testes de consistência nos dados e nos backups.</p>
Nível de DISPONIBILIDADE	Médio
Análise do nível de DISPONIBILIDADE da informação do ativo	<p>Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.</p>

## ATIVO: Portal PJ

Título do ativo	Portal PJ
Tipo do ativo	Eletrônico
Subtipo do ativo	Sistema de gestão
Descrição do ativo	PORTAL DE ADM DO CLIENTES B2B - Vendas B2B

Responsável interno do ativo	Andrea Costa
------------------------------	--------------

Nível de confiabilidade do ativo	Médio
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	Para avaliar a confidencialidade de um ativo, é necessário considerar diversos critérios que garantem a proteção dos dados contra acessos não autorizados e vazamentos. A nota foi considerada média, pois não foram identificadas as seguintes medidas: criptografia de dados em repouso para esse ativo, PENTEST periódicos e uma solução de prevenção contra perda de dados (DLP) implementada.
Nível de INTEGRIDADE	Médio
Análise do nível de INTEGRIDADE da informação do ativo	Para avaliar a integridade de um ativo, é fundamental levar em conta diversos critérios que assegurem a preservação dos dados do sistema, evitando sua corrupção, manipulação ou alteração inadequada. A nota atribuída foi média, devido à ausência das seguintes práticas: uma rotina de backup regular e confiável, testes frequentes de restauração, auditorias das alterações nos dados da aplicação, controle de acesso baseado em funções (RBAC), além da implementação de redundâncias e testes de consistência nos dados e nos backups.
Nível de DISPONIBILIDADE	Médio
Análise do nível de DISPONIBILIDADE da informação do ativo	Para avaliar a disponibilidade de um ativo de TI, é fundamental levar em conta a capacidade desse ativo de estar operacional e acessível quando necessário, evitando indisponibilidades inesperadas. A nota atribuída foi média, devido à ausência das seguintes práticas: testes regulares de recuperação de backups, testes regulares e programados do DRP e implementação de processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços.

## ATIVO: SalesForce

Título do ativo	SALESFORCE
Tipo do ativo	Eletrônico
Subtipo do ativo	CRM
Descrição do ativo	SISTEMA DE ATENDIMENTO DOS CLIENTES

Responsável interno do ativo	Flavio Goulart
------------------------------	----------------

Nível de confiabilidade do ativo	Médio
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	<p>O Salesforce é um serviço SaaS, e toda a gestão da confidencialidade do serviço é responsabilidade da fornecedora, que aplica suas próprias regras e políticas em relação a essa questão. No entanto, recomendamos que a Salesforce forneça um padrão mínimo de confidencialidade na aplicação contemplando os itens abaixo:</p> <ul style="list-style-type: none"> <li>-- Política de backup bem definida em aderência com as necessidades da CVP;</li> <li>-- Criptografia de dados em trânsito;</li> <li>-- Listas de controle de acesso (ACLs);</li> <li>-- Controle de Acesso Baseado em Funções (RBAC);</li> <li>-- MFA;</li> <li>-- DLP (prevenção contra perda de dados);</li> <li>-- Logs de Acesso;</li> <li>-- Auditoria detalhada;</li> <li>-- PENTEST periódico.</li> </ul>
Nível de INTEGRIDADE	<p>O Salesforce é um serviço SaaS, e toda a gestão da integridade do serviço é responsabilidade da fornecedora, que aplica suas próprias regras e políticas em relação a essa questão. No entanto, recomendamos que a Salesforce forneça um padrão mínimo de confidencialidade na aplicação contemplando os itens abaixo:</p> <ul style="list-style-type: none"> <li>-- Política de backup bem definida em aderência com as necessidades da CVP;</li> <li>-- Criptografia de dados em trânsito;</li> <li>-- Listas de controle de acesso (ACLs);</li> <li>-- Controle de Acesso Baseado em Funções (RBAC);</li> <li>-- MFA;</li> <li>-- DLP (prevenção contra perda de dados);</li> <li>-- Logs de Acesso;</li> <li>-- Auditoria detalhada;</li> <li>-- PENTEST periódico.</li> </ul>
Nível de DISPONIBILIDADE	<p>O Salesforce é um serviço SaaS, e toda a gestão da disponibilidade do serviço é responsabilidade da fornecedora, que aplica suas próprias regras e políticas em relação a essa questão. No entanto, recomendamos que a Salesforce forneça um padrão mínimo de confidencialidade na aplicação contemplando os itens abaixo:</p> <ul style="list-style-type: none"> <li>-- Política de backup bem definida em aderência com as necessidades da CVP;</li> <li>-- Política de recuperação bem definida em aderência com as necessidades da CVP;</li> <li>-- SLA bem definido da disponibilidade da ferramenta;</li> <li>-- Processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços;</li> <li>-- PENTEST periódico.</li> </ul>

**Nota:** Ativo contratado como SaaS. Nesse formato, a responsabilidade pela garantia da CID (Confidencialidade, Integridade e Disponibilidade) é do fornecedor, no caso, a SALESFORCE. No entanto, a CVP pode e deve exigir um padrão mínimo de segurança ao contratar um fornecedor, garantindo que a confiabilidade esteja alinhada aos moldes e à estratégia estabelecidos pela CVP.

## ATIVO: PowerBI

Título do ativo	PBI
Tipo do ativo	Eletrônico
Subtipo do ativo	Business Intelligence
Descrição do ativo	INFORMAÇÕES GERENCIAIS - Relatórios Online

Responsável interno do ativo	Leandro Branquinho
------------------------------	--------------------

Nível de confiabilidade do ativo	Médio
Nível de CONFIDENCIALIDADE	Médio
Análise do nível de CONFIDENCIALIDADE da informação do ativo	<p>O PBI é um serviço SaaS, e toda a gestão da confidencialidade do serviço é responsabilidade da fornecedora, que aplica suas próprias regras e políticas em relação a essa questão. No entanto, recomendamos que a Microsoft forneça um padrão mínimo de confidencialidade na aplicação contemplando os itens abaixo:</p> <ul style="list-style-type: none"> <li>-- Política de backup bem definida em aderência com as necessidades da CVP;</li> <li>-- Criptografia de dados em trânsito;</li> <li>-- Listas de controle de acesso (ACLs);</li> <li>-- Controle de Acesso Baseado em Funções (RBAC);</li> <li>-- MFA;</li> <li>-- DLP (prevenção contra perda de dados);</li> <li>-- Logs de Acesso;</li> <li>-- Auditoria detalhada;</li> <li>-- PENTEST periódico.</li> </ul>
Nível de INTEGRIDADE	<p>O PBI é um serviço SaaS, e toda a gestão da integridade do serviço é responsabilidade da fornecedora, que aplica suas próprias regras e políticas em relação a essa questão. No entanto, recomendamos que a Microsoft forneça um padrão mínimo de confidencialidade na aplicação contemplando os itens abaixo:</p> <ul style="list-style-type: none"> <li>-- Política de backup bem definida em aderência com as necessidades da CVP;</li> <li>-- Criptografia de dados em trânsito;</li> <li>-- Listas de controle de acesso (ACLs);</li> <li>-- Controle de Acesso Baseado em Funções (RBAC);</li> <li>-- MFA;</li> <li>-- DLP (prevenção contra perda de dados);</li> <li>-- Logs de Acesso;</li> <li>-- Auditoria detalhada;</li> <li>-- PENTEST periódico.</li> </ul>
Nível de DISPONIBILIDADE	<p>O PBI é um serviço SaaS, e toda a gestão da disponibilidade do serviço é responsabilidade da fornecedora, que aplica suas próprias regras e políticas em relação a essa questão. No entanto, recomendamos que a Microsoft forneça um padrão mínimo de confidencialidade na aplicação contemplando os itens abaixo:</p> <ul style="list-style-type: none"> <li>-- Política de backup bem definida em aderência com as necessidades da CVP;</li> <li>-- Política de recuperação bem definida em aderência com as necessidades da CVP;</li> <li>-- SLA bem definido da disponibilidade da ferramenta;</li> <li>-- Processos eficazes de detecção e gerenciamento de incidentes e ameaças para responder rapidamente a falhas e garantir a operação dos serviços;</li> <li>-- PENTEST periódico.</li> </ul>

**Nota:** Ativo contratado como SaaS. Nesse formato, a responsabilidade pela garantia da CID (Confidencialidade, Integridade e Disponibilidade) é do fornecedor, no caso, a Microsoft. No entanto, a CVP pode e deve exigir um padrão mínimo de segurança ao contratar um fornecedor, garantindo que a confiabilidade esteja alinhada aos moldes e à estratégia estabelecidos pela CVP.

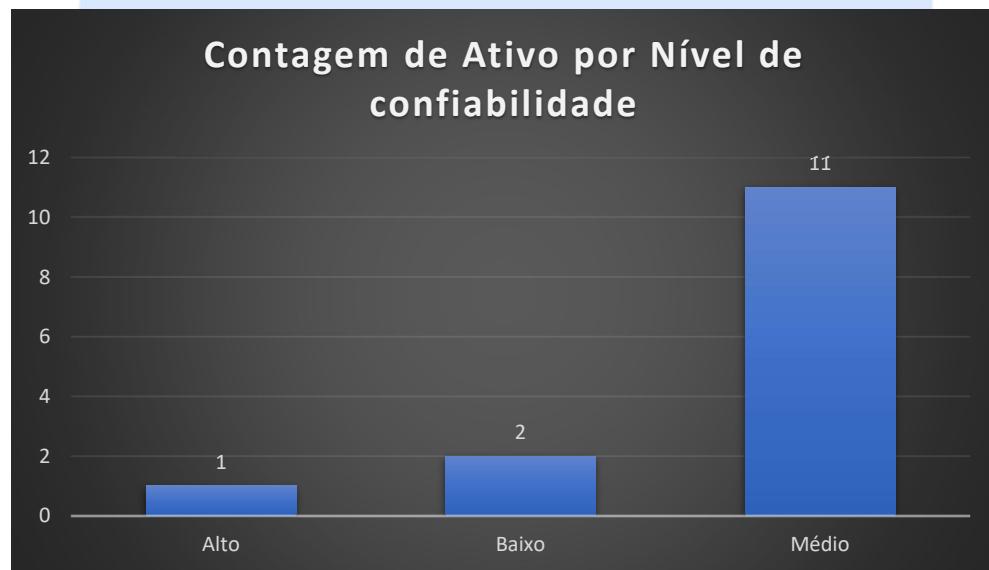
## Conclusão

De acordo com as análises detalhadas acima, concluímos que **80%** dos ativos analisados estão com nível de confiabilidade **médio**. Esse nível indica que a CVP possui medidas razoáveis e práticas para proteger dados pessoais, cumprindo os requisitos básicos da LGPD, mas pode não estar adotando as melhores práticas ou tecnologias de ponta disponíveis no mercado. O nível médio pode ser considerado suficiente para muitas empresas, dependendo da natureza e sensibilidade dos dados que estão sendo processados e armazenados.

Para a CVP, aumentar a confiabilidade dos ativos, requer a análise de algumas sugestões de medidas técnicas adicionais, tais como:

- **Detalhamento e entendimento das políticas de backup e restore:** Garantir que os procedimentos de backup e restauração sejam bem definidos e compreendidos;
- **Alta disponibilidade com replicação externa (cloud):** Implementar soluções de alta disponibilidade com replicação de dados em ambientes de nuvem;
- **Criptografia:** Utilizar criptografia avançada para proteger dados em trânsito e em repouso;
- **Controles de acesso eficazes:** Implementar e gerenciar controles de acesso rigorosos para garantir que apenas usuários autorizados possam acessar informações sensíveis;
- **Data Loss Prevention (DLP):** Adotar ferramentas de prevenção contra perda de dados para monitorar e proteger informações confidenciais;
- **Security Information and Event Management (SIEM):** Utilizar sistemas de gestão de informações e eventos de segurança para monitorar e analisar atividades de segurança em tempo real.

A implementação dessas medidas pode ajudar a CVP a aumentar a confiabilidade de seus ativos de TI, melhorando a proteção dos dados pessoais e alcançando um nível mais alto de conformidade com a LGPD. A implementação dessas medidas deve ser priorizada para os ativos com nível baixo de confiabilidade que são **SIAS** e **SMART**.



## Próximos passos

Conforme combinado entre as partes, a análise aqui detalhada agora será expandida em termos técnicos, de riscos e demais aspectos pertinentes.

Essa próxima análise será tratada entre as partes e o trabalho será planejado na sequência.